NEC

NEC Expressサーバ
Express5800シリーズ
InterSec

N8100-1017

Express5800/SG300b

ユーザーズガイド

856-124846-006-00
2005年　3月　初版

商標について

ESMPROは日本電気株式会社の登録商標です。LinuxはLinus Torvaldsの米国およびその他の国における登録商標または商標です。UNIXはThe Open Groupの登録商標です。FireWall-1はCheck Point Software Technologiesの登録商標または商標です。Microsoft、Windows、Windows Server、Windows NT、MS-DOSは米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。Intel、Pentiumは米国Intel Corporationの登録商標です。ATは米国International Business Machines Corporationの米国およびその他の国における登録商標です。DatalightとROM-DOSはDatalight, Inc.の登録商標または商標です。Adaptecとそのロゴ、HostRAID、Adaptec Storage Managerは米国Adaptec, Inc.の登録商標または商標です。Adobe、Adobeロゴ、Acrobatは、Adobe Systems Incorporated(アドビ システムズ社)の商標です。

その他、記載の会社名および商品名は各社の商標または登録商標です。

オペレーティングシステムの表記について

Windows Server 2003はMicrosoft® Windows Server™ 2003 Standard Edition operating systemおよびMicrosoft® Windows Server™ 2003 Enterprise Edition operating systemの略です。Windows 2000はMicrosoft® Windows® 2000 Server operating systemおよびMicrosoft® Windows® 2000 Advanced Server operating system、Microsoft® Windows® 2000 Professional operating systemの略称です。Windows XPはMicrosoft® Windows® XP Home Edition operating systemおよび Microsoft Windows XP Professional operating systemの略です。Windows NTはMicrosoft® Windows NT® Server network operating system version 3.51/4.0およびMicrosoft® Windows NT® Workstation operating system version 3.51/4.0の略称です。Windows MeはMicrosoft® Windows® Millennium Edition operating systemの略称です。Windows 98はMicrosoft® Windows®98 operating systemの略称です。Windows 95はMicrosoft® Windows®95 operating systemの略称です。

サンプルアプリケーションで使用している名称は、すべて架空のものです。実在する品名、団体名、個人名とは一切関係ありません。

本製品で使用しているソフトウェアの大部分は、BSDの著作とGNUのパブリックライセンスの条項に基づいて自由に配布することができます。ただし、アプリケーションの中には、その所有者に所有権があり、再配布に許可が必要なものがあります。
本製品で使用しているオープンソースコードについては弊社サイト『http://www.express.nec.co.jp/linux/』をご参照ください。

ご注意

(1) 本書の内容の一部または全部を無断転載することは禁止されています。
(2) 本書の内容に関しては将来予告なしに変更することがあります。
(3) 弊社の許可なく複製・改変などを行うことはできません。
(4) 本書は内容について万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、お買い求めの販売店にご連絡ください。
(5) 運用した結果の影響については(4)項にかかわらず責任を負いかねますのでご了承ください。

このユーザーズガイドは、必要なときすぐに参照できるよう、お手元に置いておくようにしてください。「使用上のご注意」を必ずお読みください。

⚠ 使用上のご注意 - 必ずお読みください -

本製品を安全に正しくご使用になるために必要な情報が記載されています。

安全にかかわる表示について

本製品を安全にお使いいただくために、このユーザーズガイドの指示に従って操作してください。

このユーザーズガイドには本製品のどこが危険か、どのような危険に遭うか、どうすれば危険を避けられるかなどについて説明されています。また、装置内で危険が想定される箇所またはその付近には警告ラベルが貼り付けられています(本体に印刷されている場合もあります)。

ユーザーズガイド、および警告ラベルでは、危険の程度を表す言葉として、「警告」と「注意」という用語を使用しています。それぞれの用語は次のような意味を持つものとして定義されています。

⚠ 警告　**人が死亡する、または重傷を負うおそれがあることを示します。**

⚠ 注意　**火傷やけがなどを負うおそれや物的損害を負うおそれがあることを示します。**

危険に対する注意・表示は次の3種類の記号を使って表しています。それぞれの記号は次のような意味を持つものとして定義されています。

記号	意味	説明	例
△	**注意の喚起**	この記号は危険が発生するおそれがあることを表します。記号の中の絵表示は危険の内容を図案化したものです。	(例)(感電注意)
⃠	**行為の禁止**	この記号は行為の禁止を表します。記号の中や近くの絵表示は、してはならない行為の内容を図案化したものです。	(例)(分解禁止)
●	**行為の強制**	この記号は行為の強制を表します。記号の中の絵表示は、しなければならない行為の内容を図案化したものです。危険を避けるためにはこの行為が必要です。	(例)(プラグを抜け)

(ユーザーズガイドでの表示例)

本書と警告ラベルで使用する記号とその内容

注意の喚起

記号	内容	記号	内容
	感電のおそれのあることを示します。		発煙または発火のおそれがあることを示します。
	指がはさまれてけがをするおそれがあることを示します。		けがをするおそれがあることを示します。
	高温による傷害を負うおそれがあることを示します。		特定しない一般的な注意・警告を示します。
	爆発や破裂による傷害を負うおそれがあることを示します。		

行為の禁止

記号	内容	記号	内容
	特定しない一般的な禁止を示します。		本装置を分解・修理・改造しないでください。感電や火災のおそれがあります。
	火気に近づけないでください。発火するおそれがあります。		ぬれた手で触らないでください。感電するおそれがあります。
	指定された場所には触らないでください。感電や火傷などの傷害のおそれがあります。		水や液体がかかる場所で使用しないでください。水にぬらすと感電や発火のおそれがあります。

行為の強制

記号	内容	記号	内容
	本装置の電源プラグをコンセントから抜いてください。火災や感電のおそれがあります。		特定しない一般的な使用者の行為を指示します。説明に従った操作をしてください。
	必ず接地してください。感電や火災のおそれがあります。		

安全上のご注意

本装置を安全にお使いいただくために、ここで説明する注意事項をよく読んでご理解し、安全にご活用ください。記号の説明についてはiiiページの『安全にかかわる表示について』の説明を参照してください。

全般的な注意事項

警告

人命に関わる業務や高度な信頼性を必要とする業務には使用しない

本装置は、医療機器・原子力設備や機器、航空宇宙機器・輸送設備や機器など、人命に関わる設備や機器および高度な信頼性を必要とする設備や機器などへの組み込みやこれらの機器の制御などを目的とした使用は意図されておりません。これら設備や機器、制御システムなどに本装置を使用した結果、人身事故、財産損害などが生じても弊社はいかなる責任も負いかねます。

煙や異臭、異音がしたまま使用しない

万一、煙、異臭、異音などが生じた場合は、ただちに電源をOFFにして電源プラグをコンセントから抜いてください。その後、お買い求めの販売店または保守サービス会社にご連絡ください。そのまま使用すると火災の原因となります。

針金や金属片を差し込まない

通気孔やフロッピーディスクドライブ、CD-ROMドライブのすきまから金属片や針金などの異物を差し込まないでください。感電の危険があります。

規格以外のラックで使用しない

本装置はEIA規格に適合した19型(インチ)ラックにも取り付けて使用できます。EIA規格に適合していないラックに取り付けて使用しないでください。本装置が正常に動作しなくなるばかりか、けがや周囲の破損の原因となることがあります。本装置で使用できるラックについては保守サービス会社にお問い合わせください。

指定以外の場所で使用しない

本装置を取り付けるラックを設置環境に適していない場所には設置しないでください。
本装置やラックに取り付けているその他のシステムに悪影響をおよぼすばかりでなく、火災やラックの転倒によるけがなどをするおそれがあります。設置場所に関する詳細な説明や耐震工事についてはラックに添付の説明書を読むか保守サービス会社にお問い合わせください。

⚠注意

海外で使用しない

本装置は、日本国内専用の装置です。海外では使用できません。この装置を海外で使用すると火災や感電の原因となります。

装置内に水や異物を入れない

装置内に水などの液体、ピンやクリップなどの異物を入れないでください。火災や感電、故障の原因となります。もし入ってしまったときは、すぐ電源をOFFにして、電源プラグをコンセントから抜いてください。分解しないで販売店または保守サービス会社にご連絡ください。

ラックの設置・取扱いに関する注意事項

⚠注意

1人で搬送・設置をしない

ラックの搬送・設置は2人以上で行ってください。ラックが倒れてけがや周囲の破損の原因となります。特に高さのあるラック(44Uラックなど)はスタビライザなどによって固定されていないときは不安定な状態にあります。かならず2人以上でラックを支えながら搬送・設置をしてください。

荷重が集中してしまうような設置はしない

ラック、および取り付けたデバイスの重量が一点に集中しないようスタビライザを取り付けるか、複数台のラックを連結して荷重を分散してください。ラックが倒れてけがをするおそれがあります。

1人で部品の取り付けをしない

ラック用のドアやトレーなどの部品は2人以上で取り付けてください。部品を落として破損させるばかりでなく、けがをするおそれがあります。

ラックが不安定な状態でデバイスをラックから引き出さない

ラックから装置を引き出す際は、必ずラックを安定させた状態(スタビライザの設置や耐震工事など)で引き出してください。

複数台のデバイスをラックから引き出した状態にしない

複数台のデバイスをラックから引き出すとラックが倒れるおそれがあります。装置は一度に1台ずつ引き出してください。

定格電源を超える配線をしない

やけどや火災、装置の損傷を防止するためにラックに電源を供給する電源分岐回路の定格負荷を超えないようにしてください。電気設備の設置や配線に関しては、電源工事を行った業者や管轄の電力会社にお問い合わせください。

電源・電源コードに関する注意事項

警告

ぬれた手で電源プラグを持たない

ぬれた手で電源プラグの抜き差しをしないでください。感電するおそれがあります。

アース線をガス管につながない

アース線は絶対にガス管につながないでください。ガス爆発の原因になります。

注意

指定以外のコンセントに差し込まない

指定された電圧で指定のコンセントをお使いください。指定以外で使うと火災や漏電の原因となります。
また、延長コードが必要となるような場所には設置しないでください。本装置の電源仕様に合っていないコードに接続すると、コードが過熱して火災の原因となります。

たこ足配線にしない

コンセントに定格以上の電流が流れることによって、過熱して火災の原因となるおそれがあります。

中途半端に差し込まない

電源プラグは根元までしっかりと差し込んでください。中途半端に差し込むと接触不良のため発熱し、火災の原因となることがあります。また差し込み部にほこりがたまり、水滴などが付くと発熱し、火災の原因となるおそれがあります。

指定以外の電源コードを使わない

本装置に添付されている電源コード以外のコードを使わないでください。電源コードに定格以上の電流が流れると、火災の原因となるおそれがあります。
また、電源コードの破損による感電や火災を防止するために次の注意をお守りください。

- コード部分を引っ張らない。
- 電源コードを折り曲げない。
- 電源コードをねじらない。
- 電源コードを踏まない。
- 電源コードを束ねたまま使わない。
- 電源コードをステープラなどで固定しない。
- 電源コードをはさまない。
- 電源コードに薬品類をかけない。
- 電源コードの上にものを載せない。
- 電源コードを改造・加工・修復しない。
- 損傷した電源コードを使わない。（損傷した電源コードはすぐ同じ規格の電源コードと取り替えてください。交換に関しては、お買い求めの販売店または保守サービス会社にご連絡ください。）

添付の電源コードを他の装置や用途に使用しない

添付の電源コードは本装置に接続し、使用することを目的として設計され、その安全性が確認されている物です。決して他の装置や用途に使用しないでください。火災や感電の原因となるおそれがあります。

設置・移動・保管・接続に関する注意事項

⚠ 注意

指定以外の場所に設置・保管しない

本装置を次に示すような場所や本書で指定している場所以外に置かないでください。火災の原因となるおそれがあります。

- ほこりの多い場所。
- 給湯器のそばなど湿気の多い場所。
- 直射日光が当たる場所。
- 不安定な場所。

腐食性ガスの存在する環境で使用しない

腐食性ガス（塩化ナトリウムや二酸化硫黄、硫化水素、二酸化窒素、塩素、アンモニア、オゾンのど）の発生する場所に設置し、使用しないでください。また、ほこり中に腐食を促進する成分（硫黄など）や導電性の金属などが含まれている環境へも設置しないでください。装置内部のプリント板が腐食・ショートし、火災の原因となるおそれがあります。

落下注意

本装置をラックに取り付けるまたは取り外す際は、底面をしっかり持ってください。ラック取り付けブラケットには、落下・脱落防止（ストッパ/ロック）機構がないため装置をラックからすべて引き出すと、装置がラックから外れて落下してけがをするおそれがあります。

装置を引き出した状態にしない

装置を引き出した状態のまま作業をしないでください。ラック取り付けブラケットには落下・脱落防止(ストッパ/ロック)機構がないため作業中に装置が脱落してけがをするおそれがあります。

カバーを外したまま取り付けない

本装置のカバー類を取り外した状態でラックに取り付けないでください。装置内部の冷却効果を低下させ、誤動作の原因となるばかりでなく、ほこりが入って火災や感電の原因となることがあります。

指を挟まない

ラックへの取り付け・取り外しの際にレールなどで指を挟んだり、切ったりしないよう十分注意してください。

プラグを差し込んだままインタフェースケーブルの取り付けや取り外しをしない

インタフェースケーブルの取り付け/取り外しは電源コードをコンセントから抜いて行ってください。たとえ電源をOFFにしても電源コードを接続したままケーブルやコネクタに触ると感電したり、ショートによる火災を起こしたりすることがあります。

⚠注意

指定以外のインタフェースケーブルを使用しない

インタフェースケーブルは、弊社が指定するものを使用し、接続する装置やコネクタを確認した上で接続してください。指定以外のケーブルを使用したり、接続先を誤ったりすると、ショートにより火災を起こすことがあります。
また、インタフェースケーブルの取り扱いや接続について次の注意をお守りください。

- 破損したケーブルコネクタを使用しない。
- ケーブルを踏まない。
- ケーブルの上にものを載せない。
- ケーブルの接続がゆるんだまま使用しない。
- 破損したケーブルを使用しない。

お手入れ・内蔵機器の取り扱いに関する注意事項

自分で分解・修理・改造はしない

本書に記載されている場合を除き、絶対に分解したり、修理・改造を行ったりしないでください。装置が正常に動作しなくなるばかりでなく、感電や火災の危険があります。

リチウムバッテリを取り外さない

本装置内部にはリチウムバッテリが取り付けられています。リチウムバッテリを取り外さないでください。リチウムバッテリは火を近づけたり、水に浸けたりすると爆発するおそれがあります。

また、リチウムバッテリの寿命で装置が正しく動作しなくなったときは、ご自分で分解・交換・充電などをせずにお買い求めの販売店、または保守サービス会社に連絡してください。

プラグを差し込んだまま取り扱わない

お手入れや本装置内蔵用オプションの取り付け/取り外し、装置内ケーブルの取り付け/取り外しは、本装置の電源をOFFにして、電源プラグをコンセントから抜いて行ってください。たとえ電源をOFFにしても、電源コードを接続したまま装置内の部品に触ると感電するおそれがあります。
また、電源プラグはときどき抜いて、乾いた布でほこりやゴミをよくふき取ってください。ほこりがたまったままで、水滴などが付くと発熱し、火災の原因となるおそれがあります。

⚠ 注意

高温注意

本装置の電源をOFFにした直後は、内蔵型のハードディスクドライブなどをはじめ装置内の部品が高温になっています。十分に冷めたことを確認してから取り付け/取り外しを行ってください。

中途半端に取り付けない

電源ケーブルやインタフェースケーブル、ボードは確実に取り付けてください。中途半端に取り付けると接触不良を起こし、発煙や発火の原因となるおそれがあります。

コネクタカバーを取り付けずに使用しない

内蔵デバイスと接続していない電源ケーブルのコネクタにはコネクタカバーが取り付けられています。使用しないコネクタにはコネクタカバーを取り付けてください。コネクタカバーを取り付けずに使用すると、コネクタが内部の部品に接触して火災や感電の原因となります。

運用中の注意事項

⚠ 注意

雷が鳴ったら触らない

雷が発生しそうなときは電源プラグをコンセントから抜いてください。また電源プラグを抜く前に、雷が鳴りだしたら、ケーブル類も含めて装置には触れないでください。火災や感電の原因となります。

ペットを近づけない

本装置にペットなどの生き物を近づけないでください。排泄物や体毛が装置内部に入って火災や感電の原因となります。

CD-ROMドライブのトレーを引き出したまま放置しない

引き出したトレーの間からほこりが入り誤動作を起こすおそれがあります。また、トレーにぶつかりけがをするおそれがあります。

近くで携帯電話やPHS、ポケットベルを使わない

本装置のそばでは携帯電話やPHS、ポケットベルの電源をOFFにしておいてください。電波による誤動作の原因となります。

動作中に装置をラックから引き出さない

本装置が動作しているときにラックから引き出したり、ラックから取り外したりしないでください。装置が正しく動作しなくなるばかりでなく、ラックから外れてけがをするおそれがあります。

巻き込み注意

本装置の動作中は背面にある冷却ファンの部分に手や髪の毛を近づけないでください。手をはさまれたり、髪の毛が巻き込まれたりしてけがをするおそれがあります。

警告ラベルについて

本体内の危険性を秘める部品やその周辺には警告ラベルが表示されています（警告ラベルは本体に印刷されているか、貼り付けられている場合があります）。これは本体を取り扱う際、考えられる危険性を常にお客様に意識していただくためのものです（ラベルをはがしたり、塗りつぶしたり、汚したりしないでください）。もしこのラベルが貼り付けられていない、はがれかかっている、汚れている、本体に印刷されていないなどしているときは販売店にご連絡ください。

取り扱い上のご注意

本装置を正しく動作させるために次に示す注意事項をお守りください。これらの注意を無視した取り扱いをすると本装置の誤動作や故障の原因となります。

- 周辺機器へのケーブルの接続/取り外しは本体の電源をOFFになっていることを確認し、電源コードをコンセントから外した後に行ってください。
- 電源のOFFやフロッピーディスクの取り出しは、本体のアクセスランプが消灯しているのを確認してから行ってください。
- 本体の電源を一度OFFにした後、再びONにするときは10秒以上経過してからにしてください。無停電電源装置(UPS)に接続している場合も10秒以上経過してからONになるようにスケジューリングの設定をしてください。
- 本体を移動する前に電源をOFFにして、電源プラグをコンセントから抜いてください。
- 定期的に本体を清掃してください(清掃は7章で説明しています)。定期的な清掃はさまざまな故障を未然に防ぐ効果があります。
- 落雷等が原因で瞬間的に電圧が低下することがあります。この対策として無停電電源装置等を使用することをお勧めします。
- CD規格に準拠しない「コピーガード付きCD」などのディスクにつきましては、CD再生機器における再生の保証はいたしかねます。
- PCIスロットに搭載したオプションのLANボードに接続したケーブルを抜くときは、コネクタのツメが手では押しにくくなっているため、マイナスドライバなどを使用してツメを押して抜いてください。その際に、マイナスドライバなどがLANポートやその他のポートを破損しないよう十分に注意してください。
- 次の条件に当てはまる場合は、運用の前にシステム時計の確認・調整をしてください。
  - 装置の輸送後
  - 装置の保管後
  - 装置の動作を保証する環境条件(温度：10℃～35℃・湿度：20%～80%)から外れた条件下で休止状態にした後

    システム時計は毎月1回程度の割合で確認してください。また、高い時刻の精度を要求するようなシステムに組み込む場合は、タイムサーバ(NTPサーバ)などを利用して運用することをお勧めします。
    システム時計を調整しても時間の経過と共に著しい遅れや進みが生じる場合は、お買い求めの販売店、または保守サービス会社に保守を依頼してください。
- 再度、運用する際、内蔵機器や本体を正しく動作させるためにも室温を保てる場所に保管することをお勧めします。
  装置を保管する場合は、保管環境条件(温度：-10℃～55℃、湿度：20%～80%)を守って保管してください(ただし、結露しないこと)。

- 本装置、内蔵型のオプション機器、バックアップ装置にセットするメディア(テープカートリッジ)などは、寒い場所から暖かい場所に急に持ち込むと結露が発生し、そのまま使用すると誤作動や故障の原因となります。保管した大切なデータや資産を守るためにも、使用環境に十分になじませてからお使いください。
  参考：　冬季(室温と10度以上の気温差)の結露防止に有効な時間
  ディスク装置：　約2～3時間
  メディア：　約1日
- オプションは本体に取り付けられるものであること、また接続できるものであることを確認してください。たとえ本体に取り付けや接続ができても正常に動作しないばかりか、本体が故障することがあります。
- オプションは弊社の純正品をお使いになることをお勧めします。他社製のメモリやハードディスクには本装置に対応したものもありますが、これらの製品が原因となって起きた故障や破損については保証期間中でも有償修理となります。

保守サービスについて

本装置の保守に関して専門的な知識を持つ保守員による定期的な診断・保守サービスを用意しています。
本装置をいつまでもよい状態でお使いになるためにも、保守サービス会社と定期保守サービスを契約されることをお勧めします。

はじめに

このたびは、NECのInterSecシリーズをお買い求めいただき、まことにありがとうございます。

本製品は、インターネットビジネスに欠かせないファイアウォール機能、キャッシュ機能、メールサービス、Webサービス、ウィルスチェック機能など、各機能をそれぞれの専用ハードウェアに集約したNECのInterSecシリーズの1つです。

コンパクトなボディに高性能と容易性を凝縮し、堅牢なセキュリティ機能が安全で高速なネットワーク環境を提供いたします。
また、セットアップのわずらわしさをまったく感じさせない専用のセットアッププログラムやマネージメントアプリケーションは、お客様の一元管理の元でさらに細やかで高度なサービスを提供します。

本製品の持つ機能を最大限に引き出すためにも、ご使用になる前に本書をよくお読みになり、装置の取り扱いを十分にご理解ください。

本書について

本書は、本製品を正しくセットアップし、使用できるようにするための手引きです。セットアップを行うときや日常使用する上で、わからないことや具合の悪いことが起きたときは、取り扱い上の安全性を含めてご利用ください。
本書は常に本体のそばに置いていつでも見られるようにしてください。

本文中の記号について

本書では巻頭で示した安全にかかわる注意記号の他に3種類の記号を使用しています。これらの記号と意味をご理解になり、装置を正しくお取り扱いください。

重要	装置の取り扱いや、ソフトウェアの操作で守らなければならない事柄や特に注意をすべき点を示します。
チェック	装置やソフトウェアを操作する上で確認をしておく必要がある点を示します。
ヒント	知っておくと役に立つ情報や、便利なことなどを示します。

本書の再購入について

もし本書を紛失された場合は、もよりの販売店、またはお買い求めの販売店にご相談ください。ユーザーズガイドは、InterSecシリーズのホームページからダウンロードすることができます。

http://nec8.com/

本書の構成について

本書は7つの章から構成されています。それぞれの章では次のような説明が記載されています。なお、巻末には付録・用語解説・索引があります。必要に応じてご活用ください。

重要

「使用上のご注意」をはじめにご覧ください

本編をお読みになる前に必ず本書の巻頭に記載されている「使用上のご注意」をお読みください。「使用上のご注意」では、本製品を安全に、正しくお使いになるために大切な注意事項が記載されています。

第1章　InterSecシリーズについて　本製品の特長や添付のソフトウェアについて説明します。

第2章　ハードウェアの取り扱いと操作　本体の設置や接続、各部の名称などシステムのセットアップを始める前や運用時に知っておいていただきたい基本的なことがらについて説明しています。

第3章　システムのセットアップ　専用ツールによるセットアップなど装置を使用できるまでの作業と注意事項を説明します。再セットアップの方法についても説明しています。

第4章　ファイアウォール機能の設定方法　管理クライアントからWebブラウザを使って本装置にアクセスし、ファイアウォールに関する設定をする方法について説明します。

第5章　保守・管理ソフトウェア　本体に添付の「EXPRESSBUILDER（SE） CD-ROM」の使い方とCD-ROMにあるツールやアプリケーションの使用方法について説明します。また、本体添付の「EXPRESSBUILDER（SE） CD-ROM」および「バックアップCD-ROM」にそれぞれ収納されている「ESMPRO/ServerManager」と「ESMPRO/ServerAgent」の使用方法については、それぞれのCD-ROMに格納されているオンラインドキュメントをご覧ください。

第6章　システムの拡張とコンフィグレーション　内蔵オプションの取り付け/取り外し方法と、BIOSの設定内容の確認と変更方法、標準装備のRAIDコントローラを使ったRAIDの設定方法などについて説明します。

第7章　故障かな？と思ったときは　「故障かな？」と思ったときは、装置の故障を疑う前に参照してください。また、この章では故障を未然に防ぐための保守のしかたやInterSecシリーズをご利用のお客様に提供しているサービスについても紹介しています。

付属品の確認

梱包箱の中には、本体以外にいろいろな付属品が入っています。添付の構成品チェックシートを参照してすべてがそろっていることを確認し、それぞれ点検してください。万一足りないものや損傷しているものがある場合は、販売店に連絡してください。

重要

付属品について

- 添付品はセットアップをするときやオプションの増設、装置が故障したときに必要となりますので大切に保管してください。
- オペレーティングシステムに添付のソフトウェア登録カードは、所定事項をご記入の上、必ず投函してください。
- フロッピーディスクが添付されている場合は、フロッピーディスクのバックアップをとってください。また、添付のディスクをマスタディスクとして大切に保管し、バックアップディスクを使用してください。
- 添付のフロッピーディスク、またはCD-ROMは使用方法を誤るとお客様のシステム環境を変更してしまうおそれがあります。使用についてご不明な点がある場合は、無理な操作をせずにお買い求めの販売店、または保守サービス会社にお問い合わせください。

第三者への譲渡について

本体または、本体に添付されているものを第三者に譲渡（または売却）するときは、次の注意を守ってください。

● 本体について

第三者へ譲渡（または売却）する場合には、使用上のご注意を一緒にお渡しください。

重要

ハードディスクドライブ内のデータについて

譲渡する装置内に搭載されているハードディスクドライブに保存されている大切なデータ（例えば顧客情報や企業の経理情報など）が第三者へ漏洩することのないようにお客様の責任において確実に処分してください。

オペレーティングシステムのコマンドなどを使用して削除すると、見た目は消去されたように見えますが、実際のデータはハードディスクドライブに書き込まれたままの状態にあります。完全に消去されていないデータは、特殊なソフトウェアにより復元され、予期せぬ用途に転用されるおそれがあります。

このようなトラブルを回避するために市販の消去用ソフトウェア（有償）またはサービス（有償）を利用し、確実にデータを処分することを強くお勧めします。データの消去についての詳細は、お買い求めの販売店または保守サービス会社にお問い合わせください。

なお、データの処分をしないまま、譲渡（または売却）し、大切なデータが漏洩された場合、その責任は負いかねます。

● 添付のソフトウェアについて

添付のソフトウェアを第三者に譲渡（売却）する場合には、以下の条件を満たす必要があります。

- 添付されているすべてのものを譲渡し、譲渡した側は一切の複製物を保持しないこと
- 各ソフトウェアに添付されている『ソフトウェアのご使用条件』の譲渡、移転に関する条件を満たすこと
- 譲渡、移転が認められていないソフトウェアについては、インストールした装置から削除した後、譲渡すること

消耗品・装置の廃棄について

■ 本体およびハードディスクドライブ、フロッピーディスク、CD-ROMやオプションのボードなどの廃棄については各自治体の廃棄ルールに従ってください。なお、本体添付の電源コードについても他の装置への転用を防ぐために、本体と一緒に廃棄してください。詳しくは、各自治体へお問い合わせください。

重要

- **本体のマザーボード上にあるバッテリの廃棄(および交換)についてはお買い求めの販売店または保守サービス会社までお問い合わせください。**
- **ハードディスクドライブやバックアップデータカートリッジ、フロッピーディスク、その他書き込み可能なメディア(CD-R/CD-RWなど)に保存されているデータは、第三者によって復元や再生、再利用されないようお客様の責任において確実に処分してから廃棄してください。個人のプライバシーや企業の機密情報を保護するために十分な配慮が必要です。**

■ 本体の部品の中には、寿命により交換が必要なものがあります(冷却ファン、本体内蔵のバッテリ、内蔵CD-ROMドライブ、フロッピーディスクドライブなど)。装置を安定して稼働させるために、これらの部品を定期的に交換することをお勧めします。交換や寿命については、お買い求めの販売店、または保守サービス会社にご連絡ください。

警告

リチウム電池を取り外さない

本装置内部にはリチウム電池が取り付けられています。リチウム電池を取り外さないでください。リチウム電池は火を近づけたり、水に浸けたりすると爆発するおそれがあります。

また、リチウム電池の寿命で装置が正しく動作しなくなったときは、ご自分で分解・交換・充電などをせずにお買い求めの販売店、または保守サービス会社に連絡してください。

マザーボード

目　次

3 システムのセットアップ

4　ファイアウォール機能の設定方法

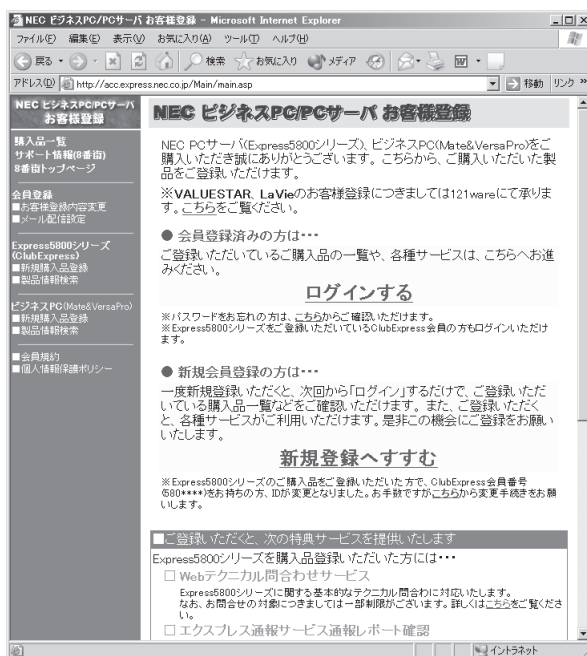
5 保守・管理ソフトウェア

6 システムの拡張とコンフィグレーション

7　故障かな?と思ったときは

ユーザー登録をしましょう！

NECでは、製品ご購入のお客様に「Club Express会員」への登録をご案内しております。添付の「お客様登録申込書」に必要事項をご記入の上、エクスプレス受付センターまでご返送いただくか、または Club Expressのインターネットホームページにてご登録ください。

http://club.express.nec.co.jp/

「Club Express会員」のみなさまには、ご希望によりExpress5800シリーズをご利用になる上で役立つ情報サービスを、無料で提供させていただきます。サービスの詳細はClub Expressのインターネットホームページにて紹介しております。ぜひ、ご覧ください。

オンラインドキュメントについて

添付の「EXPRESSBUILDER（SE） CD-ROM」には次のオンラインドキュメントが収められています。必要に応じて参照してください。

- ESMPRO/ServerManager Ver.4.1インストレーションガイド
- DianaScopeオンラインドキュメント

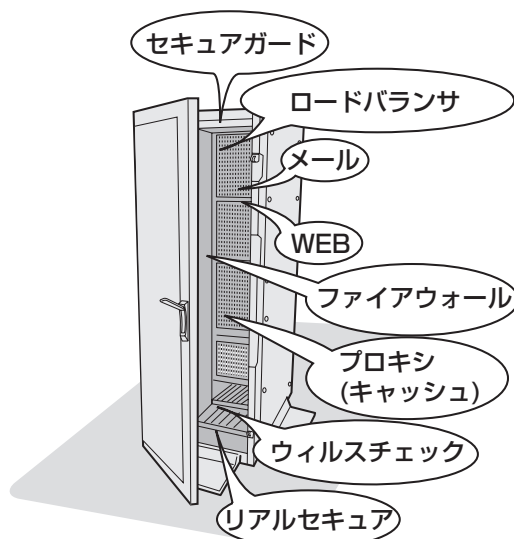
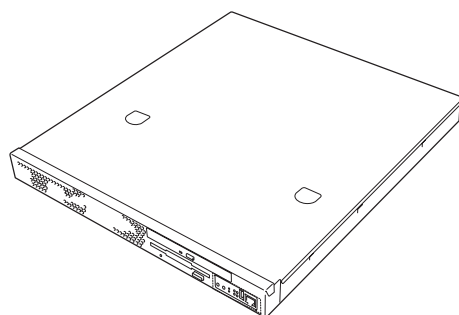
添付の「バックアップCD-ROM」にはオンラインドキュメントとして「ESMPRO/ServerAgent Ver.3.9（Linux版）」の説明書が収められています。必要に応じて参照してください。

バックアップCD-ROM:/nec/Linux/esmpo.sa/doc

1 InterSec シリーズについて

本製品や添付のソフトウェアの特長、導入の際に知っておいていただきたい事柄について説明します。

InterSecシリーズとは

「オール・イン・ワン」から「ビルドアップ」へ。
高度なセキュリティ管理により、安全かつ高速なインターネットビジネスを可能にするために生まれたのが「InterSecシリーズ」です。
お使いになる環境や用途に応じて必要となる機能を備えた装置を追加することでシステムをビルドアップすることができます。

1台のラックにそれぞれの機能を持つ装置を搭載(卓上設置も可能、またクラスタ構成可能)

InterSecシリーズの主な特長と利点は次のとおりです。

- **省スペース**

  設置スペースを最小限に抑えたコンパクトな筐体を採用。

- **運用性**

  運用を容易にする管理ツール。

- **クイックスタート**

  ウィザード形式の専用設定ツールを標準装備。短時間でセットアップを完了します。

- **高い拡張性**

  専用機として、機能ごとに単体ユニットで動作させているために用途に応じた機能拡張が容易に可能です。また、複数ユニットでクラスタ構成にすることによりシステムを拡張していくことができます。

- **コストパフォーマンスの向上**

  運用目的への最適なチューニングが行えるため、単機能の動作において高い性能を確保できます。また、単機能動作に必要な環境のみ提供できるため、余剰スペックがなく低コスト化が実現されます。

- **管理の容易性**

  環境設定や運用時における管理情報など、単機能が動作するに必要な設定のみです。そのため、導入・運用管理が容易に行えます。

InterSecシリーズには、目的や用途に応じて次のモデルが用意されています。

- **SGシリーズ(ファイアウォール)**

  インターネットと接続した中小規模の企業ネットワークを外部からの不正なアクセスから守るファイアウォール専用機です。

- **FWシリーズ(ファイアウォール)**

  CheckPoint FireWall-1を搭載し、高度なアクセス制御が可能な、大中規模の企業ネットワーク向けのファイアウォール専用機です。

- **LBシリーズ(ロードバランサ)**

  複数台のWebサーバへのトラフィック(要求)を整理し、負荷分散によるレスポンスの向上を目的とした装置です。

- **MWシリーズ(メール/WEB)**

  WebやFTPのサービスやインターネットを利用した電子メールの送受信や制御などインターネットで必要となるサービスを提供する装置です。

- **CSシリーズ(プロキシ)**

  Webアクセス要求におけるプロキシでのヒット率の向上(フォワードプロキシ)、Webサーバの負荷軽減・コンテンツ保護(リバースプロキシ)を目的とした装置です。

- **VCシリーズ(ウィルスチェック)**

  インターネット経由で受け渡しされるファイル(電子メール添付のファイルやWeb/FTPでダウンロードしたファイル)から各種ウィルスを検出/除去し、オフィスへのウィルス侵入、外部へのウィルス流出を防ぐことを目的とした装置です。

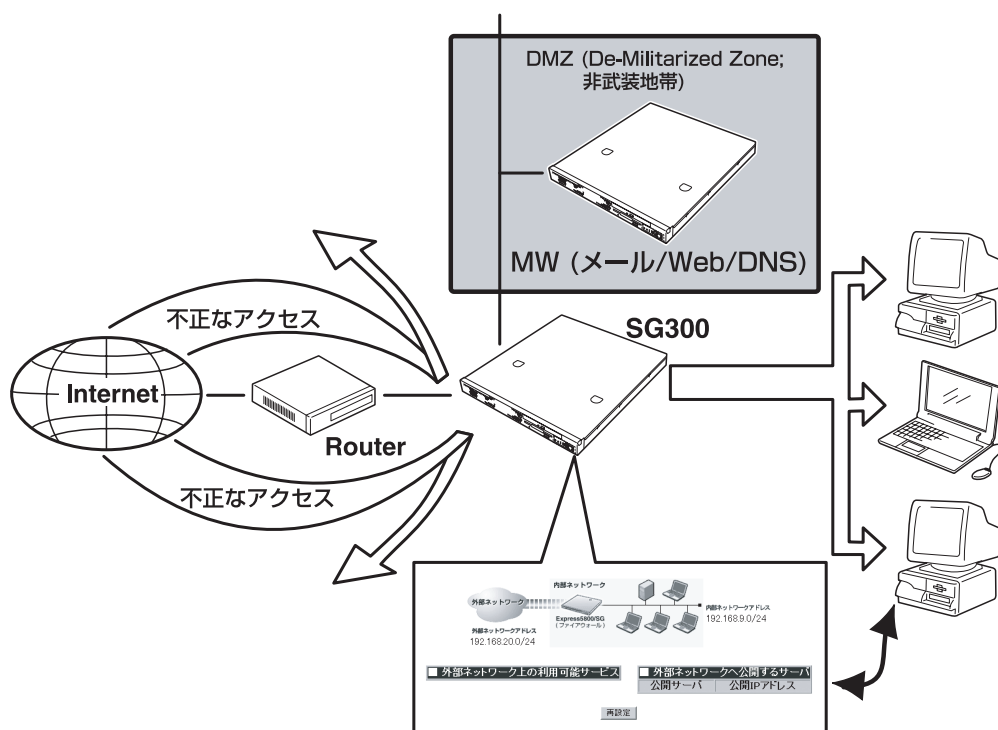
- **RSシリーズ(リアルセキュア)**

  Internet Security Systems社の不正侵入検知システムである「RealSecure Network Sensor」を搭載した装置です。ネットワークを介した外部からの侵入や攻撃、その他セキュリティ関連のイベントをリアルタイムに監視し、システムやネットワークのアクティビティを分析するセキュリティサービスを提供する装置です。

Express5800/SG300について

本装置の概略と運用に必要な情報を記します。

概　要

Express5800/SG300は、NEC独自のファイアウォールエンジンを搭載し、Virtual Private Network(VPN)機能、ホスト型IDS機能を装備したセキュリティアプライアンス機器です。
内部ネットワーク(社内LANなど)と外部ネットワーク(インターネットなど)との間のアクセスを制御し、外部からの不正な侵入を防ぎます。さらに、VPN機能による通信の暗号化やユーザ認証などを使って、インターネットなどの公衆のネットワーク上に、仮想的なユーザ専用のネットワークを実現することを可能にします。
設定・運用・管理をManagement Console(WEBベースGUI)に集約することで容易で迅速な導入を実現し、設置したその日から安全なネットワーク環境を提供します。

Management Consoleを利用してかんたんに
ポリシーを作成・編集し、セキュリティを強化可能

Express5800/SG300が提供するファイアウォールの特徴は次のとおりです。

- **アクセス制御**

  ステートフルインスペクション(通信を行うときだけ必要なポートを開く機能)により、高度なアクセス制御を可能とし、ユーザのセキュリティポリシに沿ったセキュアなネットワークを実現します。

- **アドレス変換機能(NAT/NAPT)**

 外部ネットワークと内部ネットワークとの相互通信を可能とするため、アドレス変換機能を実現しています。

- **通信量制限機能**

 ネットワークインターフェースごとに、通過するパケットの総量を制限することが可能です。これにより、アクセス過多によるサーバをダウンさせるDoS(Denial of Services)・DDoS(Distributed Denial of Services)などの攻撃が行われた場合にも、パケット量を制限し、サーバがダウンすることを防止します。

- **不正アクセス対策**

 ー オートディフェンス機能

 攻撃者は、ウェブサーバやメールサーバの持つ脆弱性をついた攻撃を行う前に、どのサーバでどのサービスが稼動しているか事前に調査(ポートスキャン)しますが、Express5800/SG300ではその事前調査活動を検出し、あたかもウェブサーバやメールサーバが数多く存在するかのように応答し、実際にサービスが稼動しているサーバの発見を困難にさせることが可能です。さらに検出後、そのホストからのアクセスを一定時間すべて破棄します。

 ー ステルススキャン検出機能

 ステルススキャンはポートスキャンと同様に、不正侵入のための前準備として行われます。通常ログなどに形跡を残さないためその発見が困難となります。Express5800/SG300では、ステルススキャン特有の正常でない通信を検出し、該当パケットの破棄とログを出力することが可能です。

 ー Ping Sweep対策機能

 不正侵入のための前準備として、どのようなホストが稼動しているか調査するために、Ping Sweepなどが行われます。Ping Sweepは、ある範囲のIPアドレス宛にpingを送出し、応答を確認することで、ホストの存在を調査するものです。Express5800/SG300では、Ping Sweepを検出し、該当パケットの破棄とログを出力することが可能です。

 ー SYN Flood対策機能

 SYN Floodは、DoS攻撃の一種で、サーバのリソースを消費し、サービスの提供をできなくする攻撃です。Express5800/SG300では、SYN Flood攻撃を検出しログを出力します。この機能により、ターゲットとなったホストを守ることが可能です。

 ー IP Spoofing対策機能

 IP Spoofingは、パケットの発信元を詐称する手法です。不正なアクセスを、あたかも内部からの許可されたアクセスであるかのように見せかけ、内部ホストに対する攻撃を可能にします。Express5800/SG300では、ルーティング情報などを元にIP Spoofingを検出し、該当パケットの破棄とログを出力することが可能です。

－　tracerouteステルス機能

あるホストまでの経路や時間を確認するために一般的に使われるtracerouteコマンドにより、経路の途中にファイアウォールが存在することを確認できます。Express5800/SG300では、tracerouteコマンドに対してもその存在を隠すことが可能です。これにより、悪意を持ったクライアントから、攻撃の対象となる可能性を低減し自分自身も守ることが可能です。

- **ユーザ管理機能**

あらかじめ定められたユーザに対してのみに、ファイアウォール機能によって守られたサービスを公開するため、その許可されたユーザ情報の管理、およびファイアウォールを通過するためのユーザ認証を行います。

- **URLフィルタリング機能**

あらかじめURLを設定しておくことで、そのWebサイトへのアクセスを制限できます。これによりインターネット上の好ましくないWebサイトや業務に関係無いWebサイトへのアクセスをブロックし、教育環境・作業効率の向上が見込めます。

- **VPN機能**

VPNとは、インターネットのような公衆のネットワーク上に、仮想的なユーザ専用のネットワークを実現する仕組みです。これにより、公衆ネットワーク上で起こりうる、通信の盗聴・改ざん・なりすましなどの危険性を排除することが可能です。Express5800/SG300では、通信相手とのLAN間接続VPNを構築することが可能であり、安価にVPN網を実現し、セキュアな通信環境を実現できます。

- **Management Console**

基本的なネットワークの設定から、ファイアウォールのセキュリティポリシの設定まで行うことのできる、統一されたウェブブラウザベースのユーザインターフェースです。

- **導入の容易性**

初期導入設定ツール、基本設定ツール、Management Console（かんたん設定/詳細設定）により、ファイアウォールなどを扱った経験の浅いユーザでも簡単に導入、運用を開始することができます。また、ネットワークインターフェースを4ポート装備しているので、ハードウェアの追加購入をすることなくDMZの構築が可能です。

- **ホットスタンバイ構成が可能**

二重化機能を標準でサポートしています。SG300を2台使用することでホットスタンバイ運用を実現し、可用性を高めます。

ライセンスキー

本製品を利用するためには、ライセンスキーの入手が必要となります。ライセンスキーを入手するためには、製品に同梱されているライセンス申請書に情報をご記入の上、ライセンス申請書に記載された宛先まで送付してください。約5営業日程度でe-mailにてライセンスキーを通知いたします。通知されたライセンスキーは重要な情報ですので、大切に保管してください。

ライセンスキーは、サポートサービス製品を購入いただき、サポートサービス申請をしていただく際にも必要な情報となります。

ソフトウェアサポートサービス

Express5800/SG300のソフトウェアおよびOSをサポートするためには以下の製品の購入が必須となります。

Exp58/SG（1年間）ソフトウェアサポートサービス

- **サービス内容**

Express5800/SG300のソフトウェアおよびOSについて、お客様(担当のNEC営業/SEを含む)からの電話、電子メールおよびFAXによる問い合わせを行うことができます。

また、インターネットを利用して、ソフトウェアおよびOSを利用可能な最新の状態へ無償でアップデートすることができます。

- **ハードウェア関するサービスは別途製品を手配いただく必要があります。**
- **ソフトウェアサポートサービスはオンサイトサービスを含んでおりません。**

- **サービス有効期間**

ユーザ登録完了後、1年間です。

ソフトウェアサポートサービスをご利用いただくには、初年度分からサポートサービス製品を手配していただく必要があります。

また、サービス有効期間終了後も継続してサービスを受けるためには、サポートサービス製品を再度ご購入いただく必要があります。

- **サービス受付時間**

弊社の営業日のうち、AM9:00～AM12:00・PM1:00～PM5:00です。

- **問い合わせ窓口のご案内**

お客様の登録が完了され次第、ご案内します。

● 問い合わせサポート範囲

Express5800/SG300にあらかじめインストールされているソフトウェアおよび添付されているNEC製のソフトウェアについてのお問い合わせに対応いたします。お客様の都合により、ソフトウェアを追加または変更した場合、本サービスの対象外となります。

● サービス開始手続き

サポートサービス製品に同梱されている「ソフトウェアサポートサービス申請書」に必要事項をご記入の上、Faxにて送付してください。申請書にはライセンスキーおよびサービス開始希望日を記入する欄などがあります。すべての項目がサービスを開始するにあたり必要な情報ですので漏れなくご記入ください。

お客様登録完了後、Express5800/SG300に投入するサポートキーおよび登録完了のお知らせが送付されます。

サポートサービスをご発注いただいてからお客様への導入時までのサービスは「暫定サポートサービス」としてサービスを提供させていただきます。ただし、暫定サポートサービス提供期間は最長3カ月とさせていただきます。

「ソフトウェアサポートサービス申請書」はお客様ごとに異なったものとなっており、複写しての使用はできません。

● 暫定サポートサービス

サポートサービス製品購入日から、ソフトウェアサポートサービス申請書にご記入いただいたサービス開始希望日までの間、暫定サポートサービスとして対応いたします。ただし、最長3カ月を限度として、技術的なQ&Aを提供します。

● サービス継続手続き

サービス有効期間(1年間)終了後もサービスを継続するためには、新規にサポートサービス製品を購入する必要があります。

また、継続のためにサポートサービス製品を購入いただいた場合には、サービス有効期間終了時にさかのぼって開始されます。前回の有効期間が切れる前にサポートサービスの購入を行ってください。

注意・制限事項

以下に示す注意・制限事項を確認の上、本装置を取り扱ってください。

- ソフトウェアアップデート機能を使用するには、ソフトウェアサポートサービスを購入し、有効なサポートキーを本製品に投入済みであることが必要です。
- ソフトウェアのアップデートを行うことで、設定画面等が本書の内容と異なる場合があります。その場合の操作方法についてはアップデート後のManagement Consoleのヘルプを参照してください。
- ユーザ認証の要求経路によって適用するルールを動的に変更することはできません。
- 設定管理用にブラウザの利用できる環境が必要です。以下のブラウザを推奨します。

  Microsoft Internet Explorer 6.0 SP1(日本語版・Windows版)
- ユーザ認証を行うには、ブラウザの利用できる環境が必要です。以下のブラウザを推奨します。

  Microsoft Internet Explorer 6.0 SP1(日本語版・Windows版)
- ユーザ認証時に、ユーザが利用している端末と本製品との間にソースアドレスを置き換えるゲートウェイが設置されている場合、そのゲートウェイを越えての認証はできません。
- システムの基本設定(インタフェースアドレス、ルーティング情報など)については必ずManagement Consoleの「基本設定」で行うか、またはシリアルコンソールからsgsetupコマンドを実行して変更してください。
- マルチキャスト通信には対応していません。
- リモートアクセスVPNにはいくつかの制限事項があります。詳細については弊社営業担当またはSEまでお問い合わせください。
- VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があるとVPN通信は行えません。
- 二重化構成でフェイルオーバが発生した場合、接続されていたセッションは切断されます。

添付のディスクについて

本装置にはセットアップや保守・管理の際に使用するCD-ROMやフロッピーディスクが添付されています。ここでは、これらのディスクに格納されているソフトウェアやディスクの用途について説明します。

重要 **添付のフロッピーディスクやCD-ROMは、システムの設定が完了した後でも、システムの再インストールやシステムの保守・管理の際に使用する場合があります。なくさないように大切に保管しておいてください。**

- **バックアップCD-ROM**

  システムのバックアップとなるCD-ROMです。

  バックアップCD-ROMには、システムのセットアップに必要なソフトウェアや各種モジュールの他にシステムの管理・監視をするための専用のアプリケーション「ESMPRO/ServerAgent」と「エクスプレス通報サービス」が格納されています。システムに備わったRAS機能を十分に発揮させるためにぜひお使いください。ESMPRO/ServerAgentの詳細な説明はバックアップCD-ROM内のオンラインドキュメントをご覧ください。エクスプレス通報サービスを使用するには別途契約が必要です。お買い求めの販売店または保守サービス会社にお問い合わせください。

- **EXPRESSBUILDER(SE) CD-ROM**

  本体およびシステムの保守・管理の際に使用するCD-ROMです。

  このCD-ROMには次のようなソフトウェアが格納されています。

  - EXPRESSBUILDER(SE)

    再セットアップの際に装置の維持・管理を行うためのユーティリティを格納するためのパーティション(保守パーティション)を作成したり、システム診断やオフライン保守ユーティリティなどの保守ツールを起動したりするときに使用します。詳細は5章を参照してください。

  - DianaScope

    システムが立ち上がらないようなときに、リモート(LAN接続またはRS-232Cケーブルによるダイレクト接続)で管理PCから本装置を管理する時に使用するソフトウェアです。詳細は5章を参照してください。

  - ESMPRO/ServerManager

    ESMPRO/ServerAgentがインストールされたコンピュータを管理します。詳細はEXPRESSBUILDER(SE)CD-ROM内のオンラインドキュメントを参照してください。

- **再インストール用ディスク(フロッピーディスク)**

  再インストールの際に使用するフロッピーディスクです。なくさないよう、大切に保管しておいてください。

- **初期導入設定用ディスク(フロッピーディスク)**

  Express5800/SG300の初期導入時の設定をするためのフロッピーディスクです。

2 ハードウェアの取り扱いと操作

本体の設置や接続、各部の名称などシステムのセットアップを始める前や運用時に知っておいていただきたい基本的なことがらについて説明します。

設　置

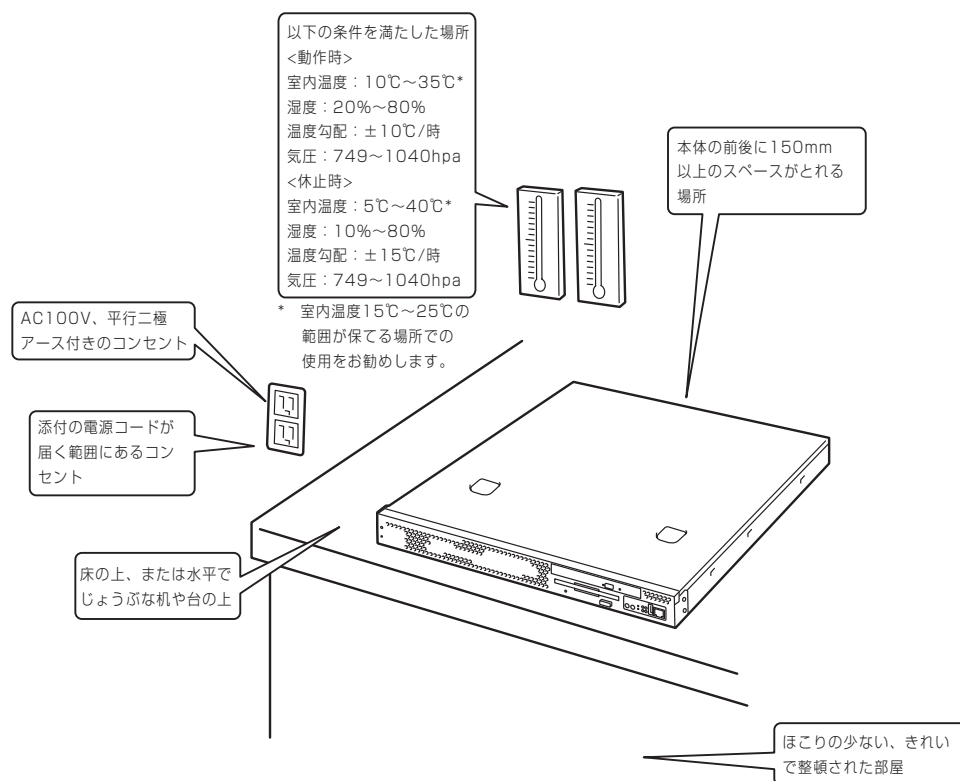
本装置は卓上またはEIA規格に適合したラックに設置して使用します。

卓上への設置

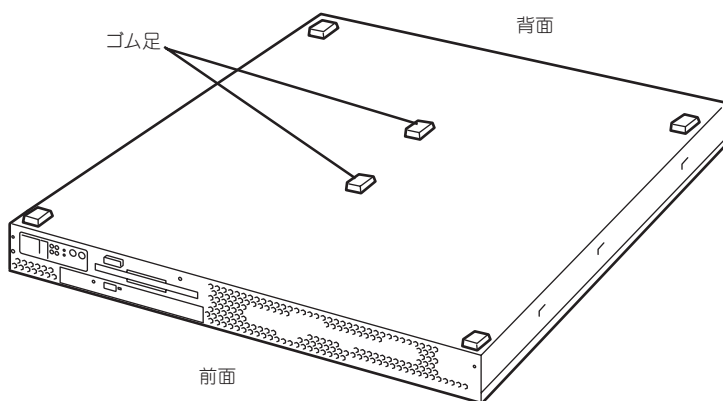
注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **指定以外の場所に設置しない**

設置にふさわしい場所は次のとおりです。

次に示す条件に当てはまるような場所には、設置しないでください。これらの場所に本体を設置すると、誤動作の原因となります。

- 温度変化の激しい場所(暖房器、エアコン、冷蔵庫などの近く)。
- 強い振動の発生する場所。
- 腐食性ガス(二酸化硫黄、硫化水素、二酸化窒素、塩素、アンモニア、オゾンなど)の存在する場所。また、ほこりや空気中に腐食を促進する成分(塩化ナトリウムや硫黄など)や導電性の金属などが含まれている場所。
- 帯電防止加工が施されていないじゅうたんを敷いた場所。
- 物の落下が考えられる場所。
- 電源コードまたはインタフェースケーブルを足で踏んだり、引っ掛けたりするおそれのある場所。
- 強い磁界を発生させるもの(テレビ、ラジオ、放送/通信用アンテナ、送電線、電磁クレーンなど)の近く(やむを得ない場合は、保守サービス会社に連絡してシールド工事などを行ってください)。
- 本体の電源コードを他の接地線(特に大電力を消費する装置など)と共用しているコンセントに接続しなければならない場所。
- 電源ノイズ(商用電源をリレーなどでON/OFFする場合の接点スパークなど)を発生する装置の近くには設置しないでください。(電源ノイズを発生する装置の近くに設置するときは電源配線の分離やノイズフィルタの取り付けなどを保守サービス会社に連絡して行ってください。)

卓上に置く場合は、本体底面に添付のゴム足を貼り付けてください。
設置場所が決まったら、本体の底面をしっかりと持って、設置場所にゆっくりと静かに置いてください。本体は3台まで積み重ねて置くことができます。

ラックへの設置

ラックの設置については、ラックに添付の説明書を参照するか、保守サービス会社にお問い合わせください。
ラックの設置作業は保守サービス会社に依頼することもできます。

警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **指定以外の場所に設置しない**
- **アース線をガス管につなjust/がない**

注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **1人で搬送・設置をしない**
- **1人で部品の取り付けをしない**
- **荷重が集中してしまうような設置はしない**
- **ラックが不安定な状態でデバイスをラックから引き出さない**
- **複数台のデバイスをラックから引き出した状態にしない**
- **定格電源を超える配線をしない**

次に示す条件に当てはまるような場所には、ラックを設置しないでください。これらの場所にラックを設置したり、ラックに本体を搭載したりすると、誤動作の原因となります。

- 本体をラックから完全に引き出せないような狭い場所。
- ラックや搭載する装置の総重量に耐えられない場所。
- スタビライザが設置できない場所や耐震工事を施さないと設置できない場所。
- 床におうとつや傾斜がある場所。
- 温度変化の激しい場所（暖房器、エアコン、冷蔵庫などの近く）。
- 強い振動の発生する場所。
- 腐食性ガス（二酸化硫黄、硫化水素、二酸化窒素、塩素、アンモニア、オゾンなど）の存在する場所。また、ほこりや空気中に腐食を促進する成分（塩化ナトリウムや硫黄など）や導電性の金属などが含まれている場所。
- 帯電防止加工が施されていないじゅうたんを敷いた場所。
- 物の落下が考えられる場所。

- 強い磁界を発生させるもの(テレビ、ラジオ、放送/通信用アンテナ、送電線、電磁クレーンなど)の近く(やむを得ない場合は、保守サービス会社に連絡してシールド工事などを行ってください)。
- 本体の電源コードを他の接地線(特に大電力を消費する装置など)と共用しているコンセントに接続しなければならない場所。
- 電源ノイズ(商用電源をリレーなどでON/OFFする場合の接点スパークなど)を発生する装置の近く(電源ノイズを発生する装置の近くに設置するときは電源配線の分離やノイズフィルタの取り付けなどを保守サービス会社に連絡して行ってください)。

本体をラックに取り付ける手順を以下に示します。取り外し手順については、取り付け手順の後で説明しています。
ここでは、NEC製のラックまたは他社製ラックへの取り付け手順について説明します。
NEC製のラックのうち、N8540-28/29/38に取り付ける場合は、オプションの「N8143-39 ラック取り付け用ブラケット」が必要です。取り付け手順については、N8143-39 ラック取り付け用ブラケットに添付の説明書を参照するか、保守サービス会社にお問い合わせください。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **規定外のラックで使用しない**
- **指定以外の場所で使用しない**

⚠注意

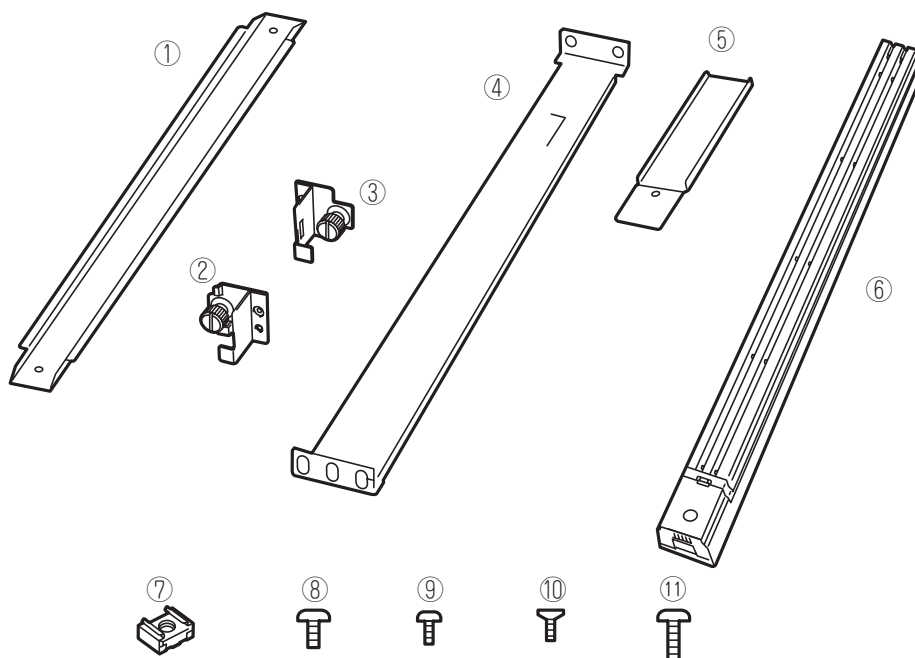
装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **落下注意**
- **装置を引き出した状態にしない**
- **カバーを外したまま取り付けない**
- **指を挟まない**

ラック内部の温度上昇とエアフローについて

複数台の装置を搭載したり、ラックの内部の通気が不十分だったりすると、ラック内部の温度が各装置から発する熱によって上昇し、動作保証温度(10℃～35℃)を超え、誤動作をしてしまうおそれがあります。運用中にラック内部の温度が保障範囲を超えないようにラック内部、および室内のエアフローについて十分な検討と対策をしてください。

取り付け部品の確認

ラックへ取り付けるために次の部品があることを確認してください。

項番	名称	数量	備考
①	マウントブラケット	2	
②	マウントホルダー(L)	1	
③	マウントホルダー(R)	1	
④	サポートブラケット	2	
⑤	エクステンションブラケット	2	
⑥	フロントベゼル	1	
⑦	コアナット	8	
⑧	ネジA	4	M4ネジ、ネジ部の長さ：6 mm、インナーレールを本体に固定する際に使用する。
⑨	ネジB	2	M3ネジ、ネジ部の長さ：6 mm、マウントホルダーを本体に固定する際に使用する。
⑩	ネジC	2	皿ネジ、M3ネジ、ネジ部の長さ：6 mm、エクステンションブラケットを固定する際に使用する。
⑪	ネジD	6	M5ネジ、ネジ部の長さ：10 mm、サポートブラケットをラックに固定する際に使用する。

必要な工具

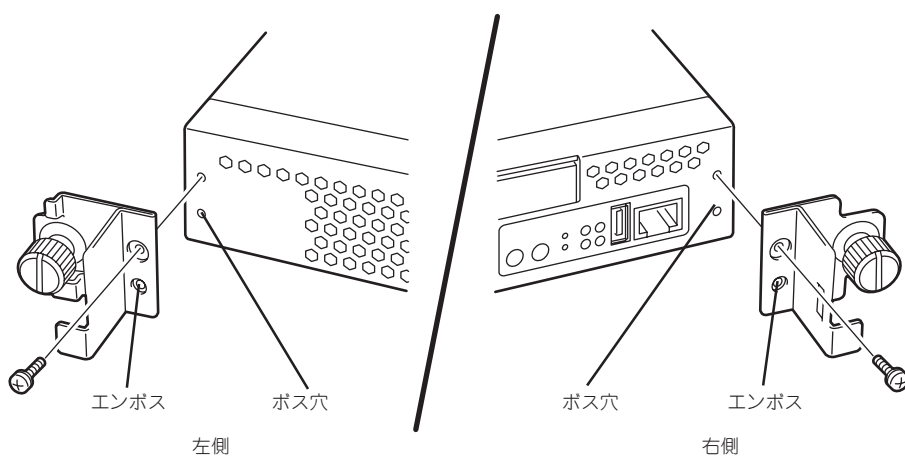
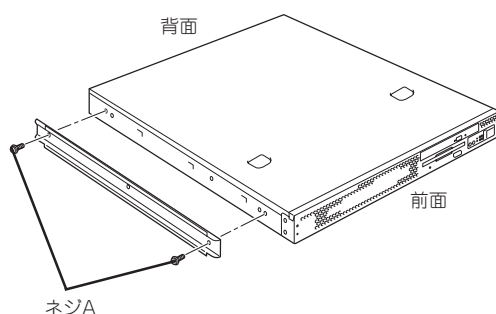
ラックへ取り付けるために必要な工具はプラスドライバとマイナスドライバです。

取り付け手順

次の手順で本体をラックへ取り付けます。

NEC製のラックのうち、N8540-28/29/38への取り付けにはN8143-39 ラック取り付け用ブラケットが必要となります。また、取り付け方法についてはN8143-39 ラック取り付け用ブラケットに添付の説明書をご覧ください。

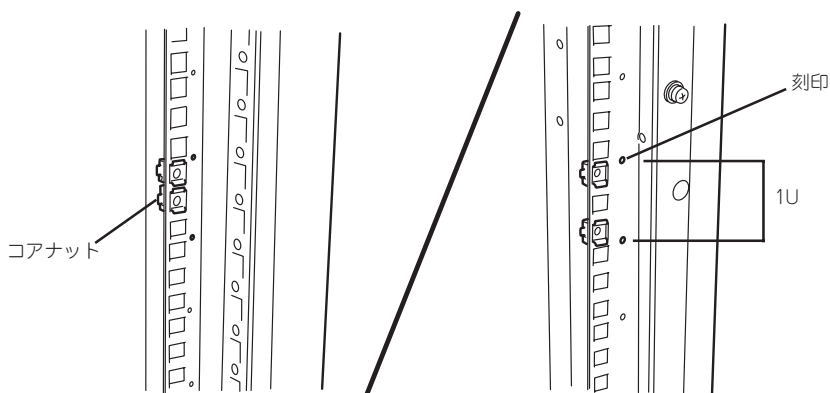
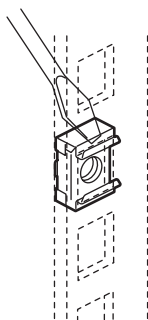
● マウントブラケットとマウントホルダーの取り付け

1. マウントブラケットのネジ穴と本体側面のネジ穴を合わせる。
2. マウントブラケットをネジA(2本)で本体に固定する。
3. もう一方の側面にマウントブラケットを手順1〜2と同じ手順で取り付ける。
4. マウントホルダーをネジB(各1本)で本体に固定する。

それぞれ、エンボスをボス穴にはめ込んでください。

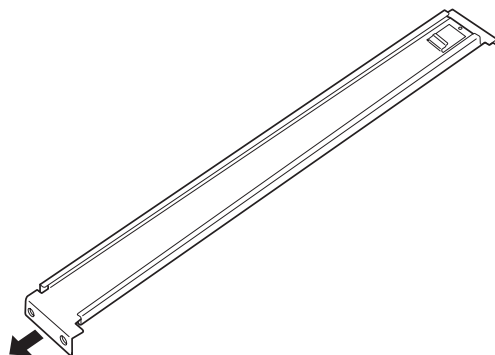
● **コアナットの取り付け**

サポートブラケットを固定する位置に添付のコアナットを取り付けます。コアナットはラックの前面(左右とも)に各2個、背面(左右とも)に各2個の合計8個取り付けます。

コアナットは「1U(ラックでの高さを表す単位)」の中に2個取り付けてください(NEC製のラックでは、1U単位に丸い刻印があります)。1Uあたり、スロット(角穴)が3つあります。3つのスロットのうち、ラック前面側では上の2つのスロットに、ラック背面側では上下のスロットにコアナットを取り付けます。

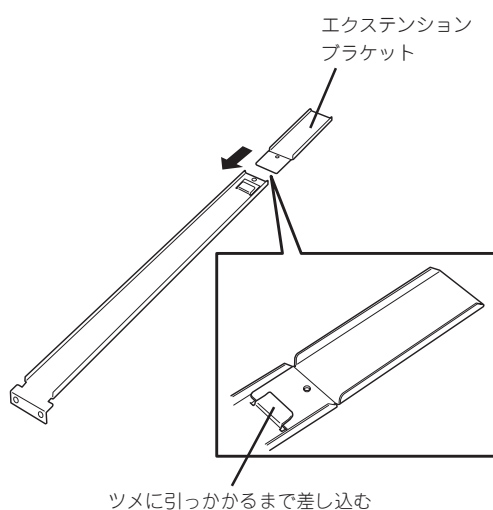
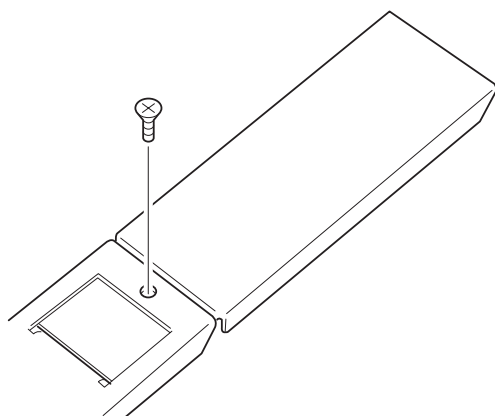
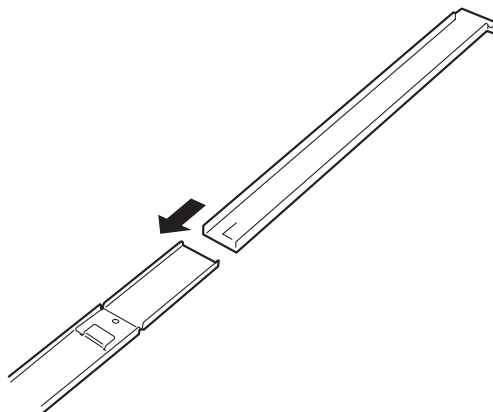
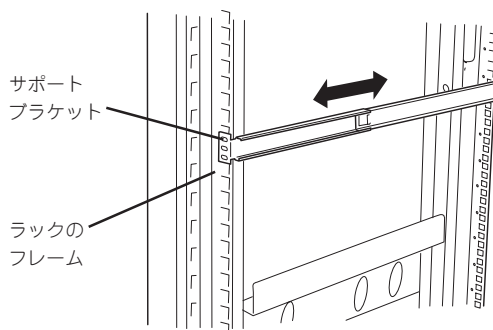
コアナットはラックの内側から取り付けます。ラックの前面に取り付けたコアナットは、上側が本体に取り付けたマウントホルダーにあるセットスクリューの受けとなります。下側はサポートブラケット前面の固定に使用します。背面のコアナットはサポートブラケット背面の固定用として使われます。

コアナットは下側のクリップをラックの四角穴に引っかけてからマイナスドライバなどで上側のクリップを穴に差し込みます。

ラックの前後、左右に取り付けたコアナットの高さが同じであることを確認してください。

● サポートブラケットの取り付け

1. サポートブラケットを引き延ばす。

2. エクステンションブラケットを取り付ける。（ラックの前後の奥行きが700mm以上の場合のみ）

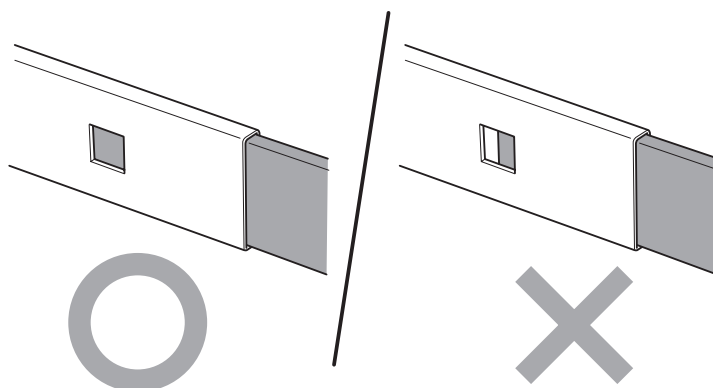
   ラックの前後の奥行きが700mm以上の場合のみ以下の手順を行います。

   ① サポートブラケットの一方を引きブラケットを分解する。

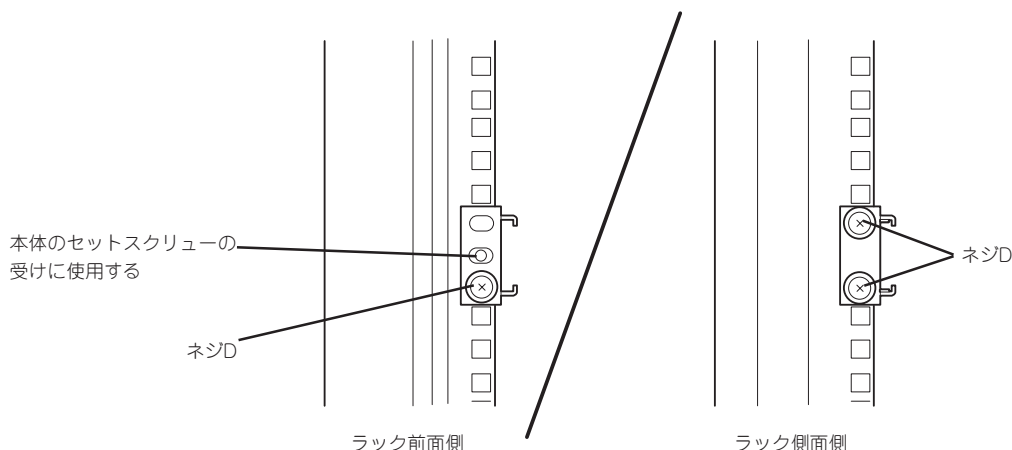
   ② エクステンションブラケットを一方のブラケットに差し込む。

   ③ エクステンションブラケットをネジC（1本）で固定する。

④ もう一方のブラケットをエクステンションブラケットに差し込む。

3. コアナットを取り付けた位置にサポートブラケット前後のフレームを合わせる。

チェック

サポートブラケットを固定する部分のフレームがラックのフレームよりも手前にあることを確認してください。

4. 一度取り外して、サポートブラケットの四角穴がブラケットで完全に隠れていることを確認する。

完全に隠れていたら、再度、ラックに取り付けてください。

5. サポートブラケットを支えながら、ネジD（3本）でラックに固定する。

サポートブラケットが水平に取り付けられていることを確認してください。

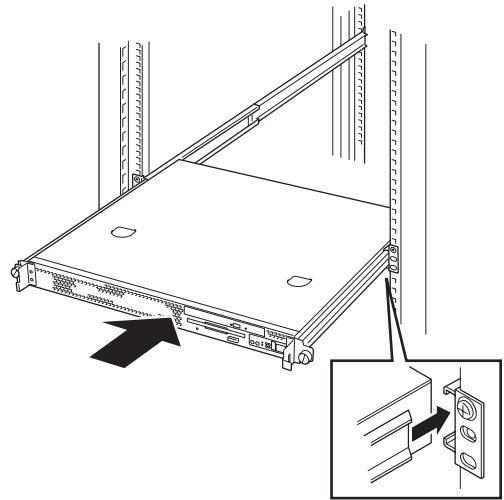
重要

サポートブラケットのネジ穴は多少上下にずらすことができる程度のクリアランスを持っています。初めて取り付ける場合は、コアナットのネジ穴がサポートブラケットのネジ穴の中央に位置するようにしてから固定してください。もし、本体を取り付けたときに本体の上下に搭載している装置にぶつかる場合は、いったん本体を取り出してサポートブラケットの固定位置を調整してください（ぶつかる装置の取り付け位置も調整する必要がある場合もあります）。

6. もう一方のサポートブラケットを手順1〜5と同じ手順で取り付ける。

すでに取り付けているサポートブラケットと同じ高さに取り付けていることを確認してください。

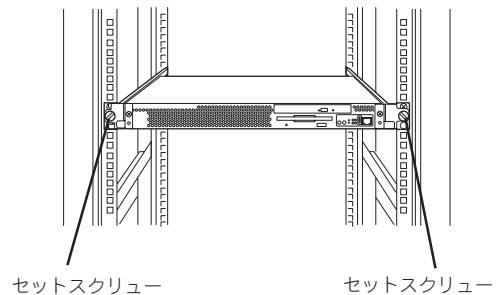
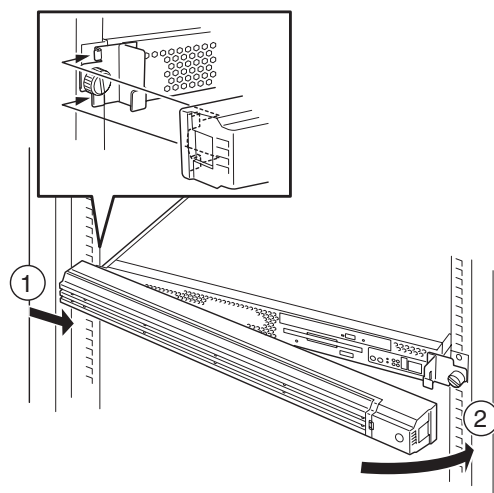
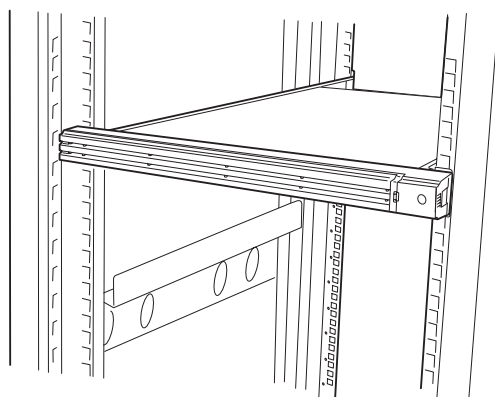
● 本体の取り付け

取り付けは1人でもできますが、ラック上段へ取り付ける場合には2人以上で行ってください。

1. 本体の前面が手前になるようにして持つ。
2. 本体側面にあるマウントブラケットをサポートブラケットに差し込みながらラックへ押し込む。

重要

本体の上下に搭載している装置にぶつかる場合は、いったん本体を取り出してサポートブラケットの固定位置を調整してください(ぶつかる装置の取り付け位置も調整する必要がある場合もあります)。

● 本体の固定

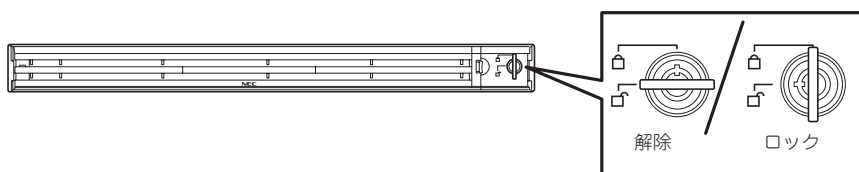
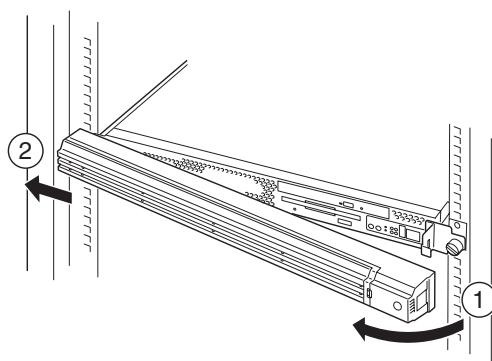
1. 本体をラックへ完全に押し込む。
2. 左右のマウントホルダーにあるセットスクリューでラックに固定する。

3. 右図を参照してフロントベゼルを取り付ける。

以上で完了です。

取り外し手順

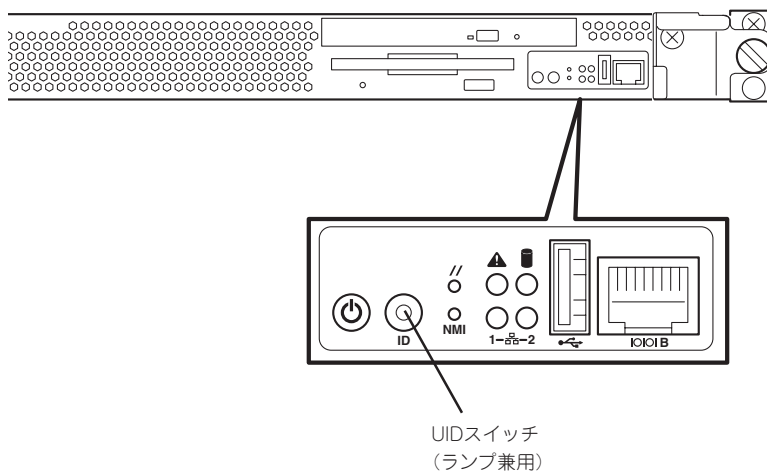
次の手順で本体をラックから取り外します。取り外しは1人でもできますが、なるべく複数名で行うことをお勧めします。

⚠ 注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **指を挟まない**
- **ラックが不安定な状態でデバイスをラックから引き出さない**
- **落下注意**
- **装置を引き出した状態にしない**
- **複数台のデバイスをラックから引き出した状態にしない**
- **動作中に装置をラックから引き出さない**

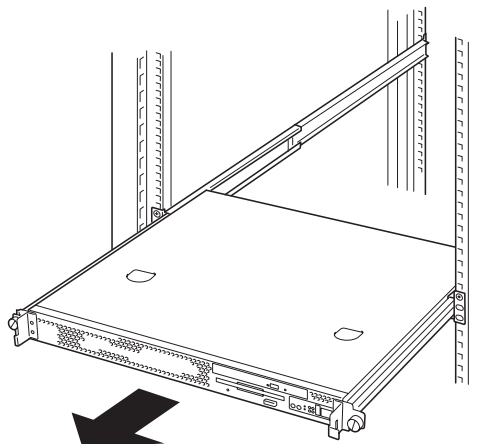
1. フロントベゼルのロックを解除する。

2. フロントベゼルを取り外す。

3. OSからシャットダウン処理をするかPOWERスイッチを押して本体の電源をOFF(POWERランプ消灯)にする。

4. 本体前面(または背面)にあるUIDスイッチを押して、UIDランプを点灯させる。

5. 本体に接続しているすべてのケーブル、および電源コードを取り外す。

チェック

本体背面のケーブルや電源コードを取り外す前にUIDランプで取り外そうとしている装置であることを確認してください。

6. 前面の左右にあるセットスクリューをゆるめて、ハンドルを持ってゆっくりとラックから引き出す。

本体の両端をしっかりと持てる位置(約15cmほど)までゆっくりと静かにラックから引き出してください。

重要

本体を引き出しすぎると、サポートブラケットから外れて落下するおそれがあります。本体に貼り付けられている警告ラベルを見ながら注意して本体を引き出してください。

7. 本体の左右底面をしっかりと持って取り外し、じょうぶで平らな机の上に置く。

重要

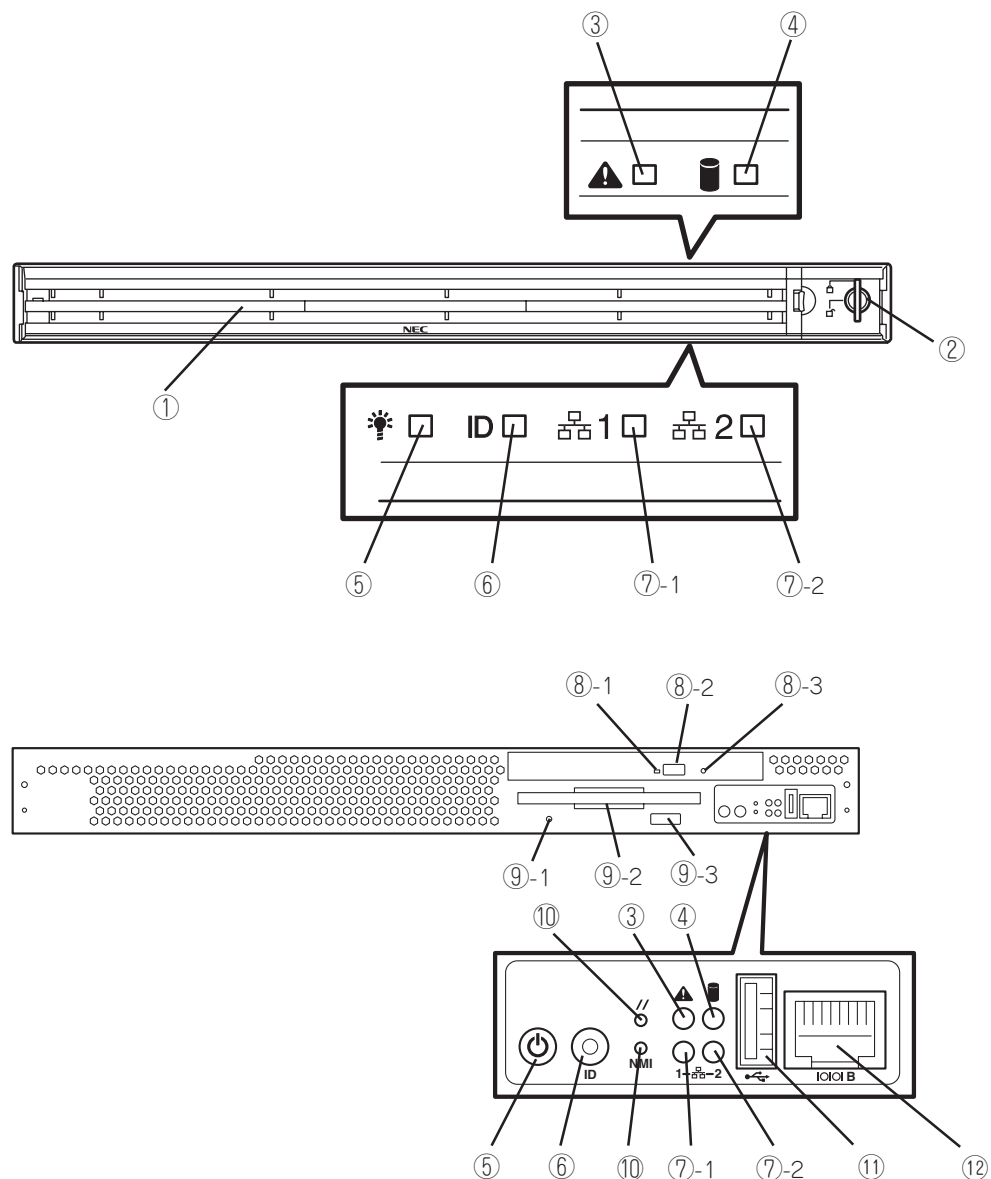
本体を引き出したまま放置しないでください。必ずラックから取り外してください。

ラックの機構部品も取り外す場合は、「取り付け手順」を参照して取り外してください。

各部の名称と機能

本体の各部の名称を次に示します。ここで説明していない部品は本装置では使用しません。

本体前面

<フロントベゼルを取り外した状態>

① フロントベゼル

日常の運用時に前面のデバイス類を保護すカバー。添付のセキュリティキーでロックすることができる(→36ページ)。

② キースロット

フロントベゼルのロックを解除するセキュリティキーの差し口。

③ STATUSランプ(緑色/アンバー色)

リモートマネージメントカードを装着時に機能する。リモートマネージメントカードが監視しているハードウェアの状態を表示するランプ。正常に動作している間は緑色に点灯する。異常が起きると消灯、緑色に点滅、またはアンバー色に点灯/点滅する(→31ページ)。

④ DISK ACCESSランプ(緑色)

取り付けているディスクが動作しているときに点灯する(→33ページ)。

⑤ リセットスイッチ

押すとリセットを実行する。通常は使用しない。

⑤ POWERスイッチ/POWERランプ(緑色)

電源をON/OFFするスイッチ(→37ページ)。一度押すとPOWERランプが点灯し、ONの状態になる。もう一度押すと電源をOFFにする(ランプは消灯する)。4秒以上押し続けると強制的にシャットダウンする。

⑥ UID(ユニットID)ランプ(青色)/UIDスイッチ

UIDランプをON/OFFにするスイッチ。スイッチを一度押すと、UIDランプが点灯し、もう一度押すと消灯する(→33ページ)。ソフトウェアからのコマンドによっても点滅する。

⑦ ACT/LINKランプ(緑色)

ネットワークポートが接続しているハブなどのデバイスとリンクしているときに緑色に点灯し、アクティブな状態にあるときに緑色に点滅する(→33ページ)。末尾の数字は「1」がLANポート1用で、「2」がLANポート4用を示す。

⑧ CD-ROMドライブ

CD-ROMの読み出しを行う装置(→40ページ)。

⑧-1 ディスクアクセスランプ

⑧-2 CDトレーイジェクトボタン

⑧-3 強制イジェクトホール

⑨ 3.5インチフロッピーディスクドライブ

3.5インチフロッピーディスクを挿入して、データの書き込み/読み出しを行う装置(→38ページ)。

⑨-1 ディスクアクセスランプ

⑨-2 ディスク挿入口

⑨-3 イジェクトボタン

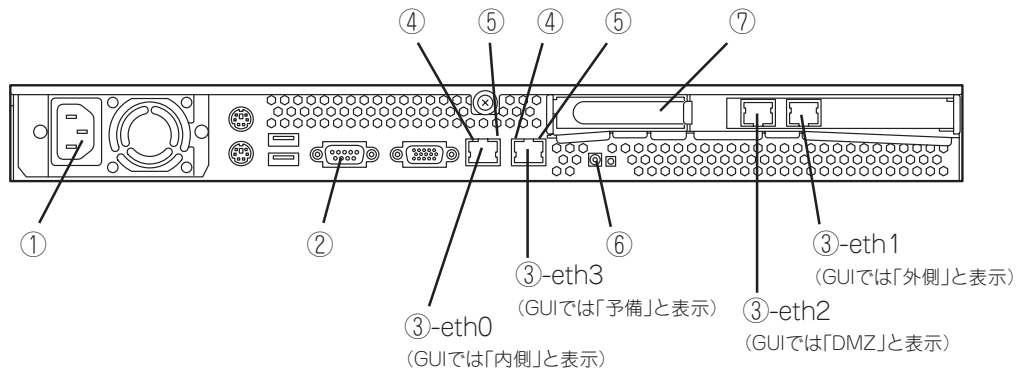
⑩ NMI(DUMP)スイッチ

押すとメモリダンプを実行する。通常は使用しない。

⑪ USBコネクタ(未使用)

⑫ シリアルポートB(COM B)コネクタ

シリアルインターフェースを持つ装置と接続する(→34ページ)。

本体背面

① **電源コネクタ**

ACコードを接続するコネクタ(→34ページ)。

② **シリアルポートA(COM A)コネクタ**

シリアルインターフェースを持つ装置と接続する(→34ページ)。

③ **LANコネクタ**

1000BASE-T/100BASE-TX/10BASE-Tと接続するコネクタ(→34ページ)。LAN上のネットワークシステムと接続する。末尾の呼称はソフトウェアからの見え方を示す。

④ **ACT/LINKランプ(緑色)**

ネットワークポートが接続しているハブなどのデバイスとリンクしているときに緑色に点灯し、アクティブな状態にあるときに緑色に点滅する(→33ページ)。

⑤ **SPEEDランプ(黄色)**

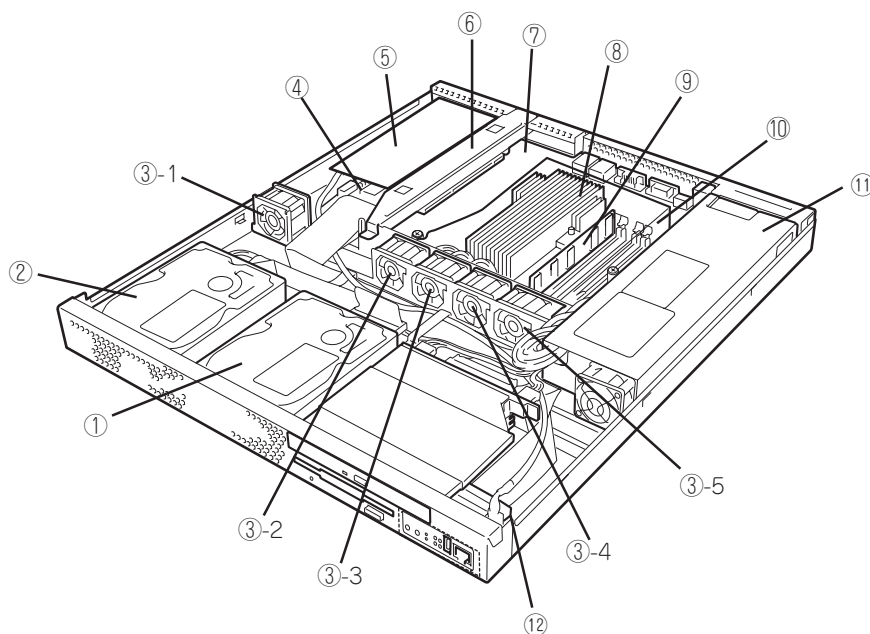
ネットワークポートの通信速度を示すランプ(→33ページ)。

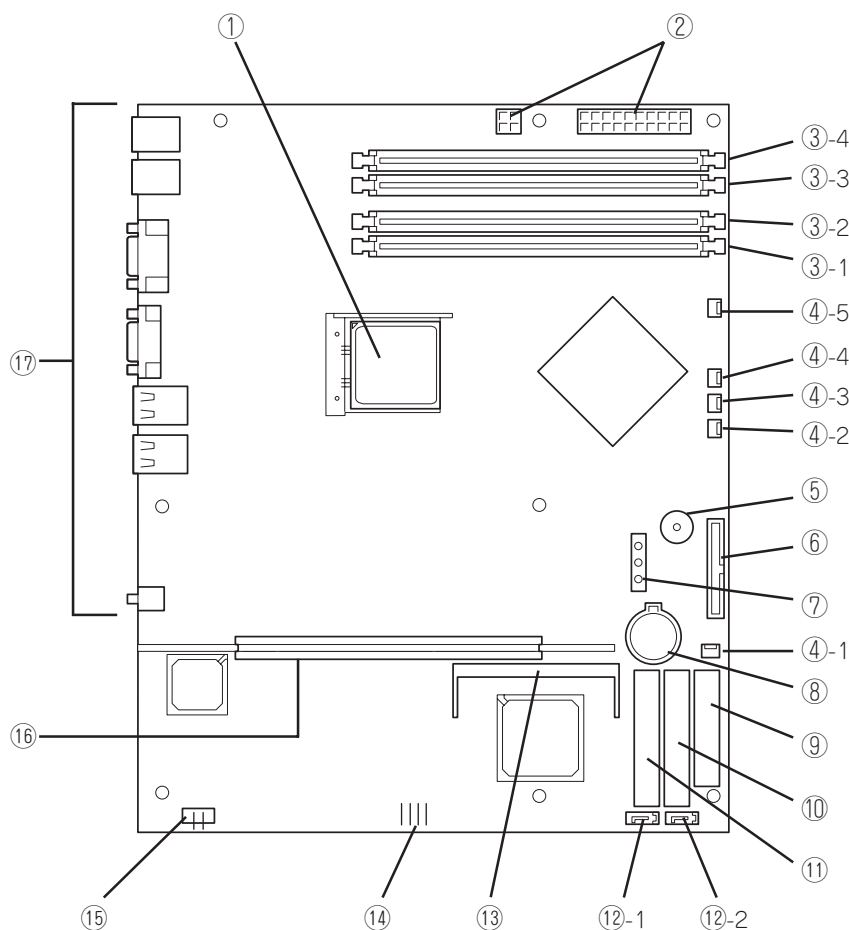
⑥ **UIDスイッチ/UIDランプ(青色)**

UIDスイッチを押したときに点灯する。ソフトウェアからのコマンドによっても点灯する。

⑦ **PCIボード増設用スロット**

オプションのPCIボードを取り付けるスロット。
標準で1000BASE-T接続ボード(2ch.、フルハイト)実装済み。

本体内部

① ドライブベイ1(ハードディスクドライブ標準装備)	⑥ PCIライザーカード
② ドライブベイ2(ハードディスクドライブはオプション)	⑦ マザーボード
③ 冷却ファン(末尾の数字はファン番号を示す)	⑧ ヒートシンク
④ リモートマネージメントカード	⑨ メモリ
⑤ ネットワークカード	⑩ エアダクト
	⑪ 電源ユニット
	⑫ フロントパネルボード

マザーボード

① プロセッサソケット
② 電源コネクタ
③ DIMMソケット(末尾の数字はDIMM番号を示す)
④ 冷却ファンコネクタ(末尾の数字はファン番号を示す)
⑤ スピーカ
⑥ フロントパネルコネクタ
⑦ CMOSメモリコンフィグレーションジャンパ
⑧ リチウムバッテリ
⑨ フロッピーディスクドライブコネクタ
⑩ IDEコネクタ(プライマリ、ハードディスク用)
⑪ IDEコネクタ(セカンダリ、未使用)
⑫ シリアルATAコネクタ(末尾の数字はコネクタ番号を示す)
⑬ リモートマネージメントカードコネクタ(N8115-01CP01を標準実装)
⑭ USBコネクタ(フロント用)
⑮ LEDコネクタ
⑯ PCIライザーカードスロット
⑰ 外部接続コネクタ/外部からの操作スイッチ

ランプ表示

本体前面には8つ、背面には3つのランプがあります。ランプの表示とその意味は次のとおりです。

POWERランプ(💡)

本体前面に1個あります。本体の電源がONの間、ランプが緑色に点灯しています。

STATUSランプ(⚠)

本体前面にあります。ハードウェアが正常に動作している間はSTATUSランプは緑色に点灯します。STATUSランプが消灯しているときや、緑色に点滅、またはアンバー色に点灯/点滅しているときはハードウェアになんらかの異常が起きたことを示します。
次にSTATUSランプの表示の状態とその意味、対処方法を示します。

- ESMPROまたはオフライン保守ユーティリティをインストールしておくとエラーログを参照することで故障の原因を確認することができます。
- いったん電源をOFFにして再起動するときに、OSからシャットダウン処理ができる場合はシャットダウン処理をして再起動してください。シャットダウン処理ができない場合はリセット、強制電源OFFをするか(382ページ参照)、一度電源コードを抜き差しして再起動させてください。

<table>
<tr><th>STATUSランプの状態</th><th>意　味</th><th>対処方法</th></tr>
<tr><td>緑色に点灯</td><td>正常に動作しています。</td><td>ー</td></tr>
<tr><td rowspan="2">緑色に点滅</td><td>メモリが縮退した状態で動作しています。</td><td>BIOSセットアップユーティリティ「SETUP」を使って縮退しているメモリを確認後、早急に交換することをお勧めします。</td></tr>
<tr><td>CPUエラーを検出した状態で動作しています。</td><td>BIOSセットアップユーティリティ「SETUP」を使ってCPUの状態を確認後、早急に交換することをお勧めします。</td></tr>
<tr><td rowspan="10">消灯</td><td>電源がOFFになっている。</td><td>電源をONにしてください。</td></tr>
<tr><td>POST中である。</td><td>しばらくお待ちください。POSTを完了後、しばらくすると緑色に点灯します。</td></tr>
<tr><td>CPUでエラーが発生した。</td><td rowspan="7">いったん電源をOFFにして、電源をONにし直してください。POSTの画面で何らかのエラーメッセージが表示された場合は、メッセージを記録して保守サービス会社に連絡してください。</td></tr>
<tr><td>CPU温度の異常を検出した。</td></tr>
<tr><td>ウォッチドッグタイマタイムアウトが発生した。</td></tr>
<tr><td>メモリで訂正不可能なエラーが検出された。</td></tr>
<tr><td>PCIシステムエラーが発生した。</td></tr>
<tr><td>PCIパリティエラーが発生した。</td></tr>
<tr><td>CPUバスエラーが発生した。</td></tr>
<tr><td>メモリダンプリクエスト中。</td><td>ダンプを採取し終わるまでお待ちください。</td></tr>
<tr><td rowspan="2">アンバー色に点灯</td><td>温度異常を検出した。</td><td>内部のファンにホコリやチリが付着していないかどうか確認してください。また、内部ファンのケーブルが確実に接続されていることを確認してください。
それでも表示が変わらない場合は、保守サービス会社に連絡してください。</td></tr>
<tr><td>電圧異常を検出した。</td><td>保守サービス会社に連絡してください。</td></tr>
<tr><td rowspan="3">アンバー色に点滅</td><td>ファンアラームを検出した。</td><td>内部ファンのケーブルが確実に接続されていることを確認してください。それでも表示が変わらない場合は、保守サービス会社に連絡してください。</td></tr>
<tr><td>温度警告を検出した。</td><td>内部のファンにホコリやチリが付着していないかどうか確認してください。また、内部ファンのケーブルが確実に接続されていることを確認してください。
それでも表示が変わらない場合は、保守サービス会社に連絡してください。</td></tr>
<tr><td>電圧警告を検出した。</td><td>保守サービス会社に連絡してください。</td></tr>
</table>

DISK ACCESSランプ()

本体前面にあります。DISK ACCESSランプは本体内部のハードディスクやCD-ROMドライブにアクセスしているときに点灯します。

アクセスランプ

本体前面にあるフロッピーディスクドライブとCD-ROMドライブのアクセスランプは、それぞれにセットされているディスクやCD-ROMにアクセスしているときに点灯します。

UID(ユニットID)ランプ

本体前面と背面に各1個あります。本体前面にあるUIDスイッチを押すと点灯しもう一度押すと消灯します。ソフトウェアからのコマンドを受信したときは点滅で表示します。複数台の装置がラックに搭載された中から特定の装置を識別したいときなどに使用することができます。特にラック背面からのメンテナンスのときは、このランプを点灯させておくと、対象装置を間違えずに作業することができます。

ACT/LINKランプ(1 、2)

本体前面と背面(LANコネクタ部分)に各1個あります。本体標準装備のネットワークポートの状態を表示します。本体とHUBに電力が供給されていて、かつ正常に接続されている場合に点灯します(LINK)。ネットワークポートが送受信を行っているときに点滅します(ACT)。LINK状態なのにランプが点灯しない場合は、ネットワークケーブルやケーブルの接続状態を確認してください。それでもランプが点灯しない場合は、ネットワーク(LAN)コントローラが故障している場合があります。お買い求めの販売店、または保守サービス会社に連絡してください。

SPEEDランプ

本体背面のLANコネクタ部分に各1個あります。本体標準装備のネットワークポートの通信モードが1000BASE-Tか、100BASE-TX、10BASE-Tのどちらのネットワークインタフェースで動作されているかを示します。アンバー色に点灯しているときは1000BASE-Tで、緑色に点灯しているときは100BASE-TXで動作されていることを示します。消灯しているときは、10BASE-Tで動作していることを示します。

接続について

本体にネットワークを接続します。
ネットワークケーブルを本体に接続してから添付の電源コードを本体に接続し、電源プラグをコンセントにつなげます。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- ぬれた手で電源プラグを持たない
- アース線をガス管につながない

⚠注意

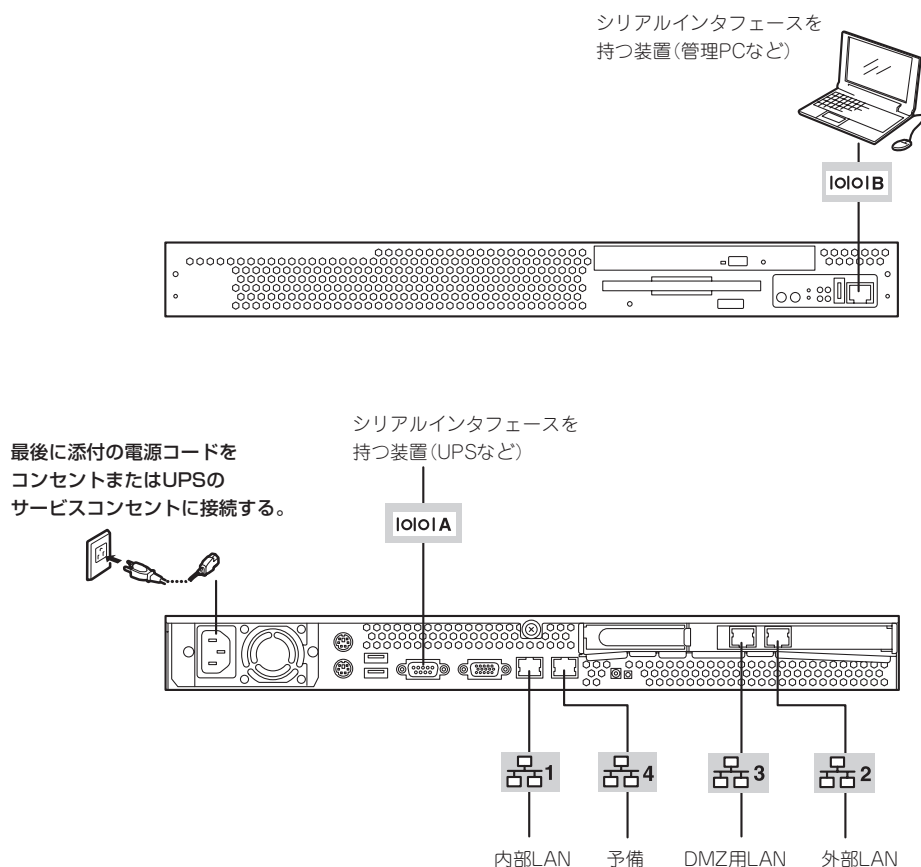
装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 指定以外のコンセントに差し込まない
- たこ足配線にしない
- 中途半端に差し込まない
- 指定以外の電源コードを使わない
- プラグを差し込んだままインタフェースケーブルの取り付けや取り外しをしない
- 指定以外のインタフェースケーブルを使用しない

重要

- 本体および接続する周辺機器の電源をOFFにしてから接続してください。ONの状態のまま接続すると誤動作や故障の原因となります。
- サードパーティの周辺機器およびインタフェースケーブルを接続する場合は、お買い求めの販売店でそれらの装置が本装置で使用できることをあらかじめ確認してください。サードパーティの装置の中には本装置で使用できないものがあります。
- ダイヤルアップ経由のエクスプレス通報サービスを使用する場合は、NECフィールディングに相談してください。
- 回線に接続する場合は、設定機関に申請済みのボードを使用してください。
- シリアルポートコネクタには専用回線を直接接続することはできません。
- PCIスロットに搭載したオプションのLANボードに接続したケーブルを抜くときは、コネクタのツメが手では押しにくくなっているため、マイナスドライバなどを使用してツメを押して抜いてください。その際に、マイナスドライバなどがLANポートやその他のポートを破損しないよう十分に注意してください。

ケーブルを接続した後は、ケーブルタイなどでケーブルが絡まないように束ねてください。

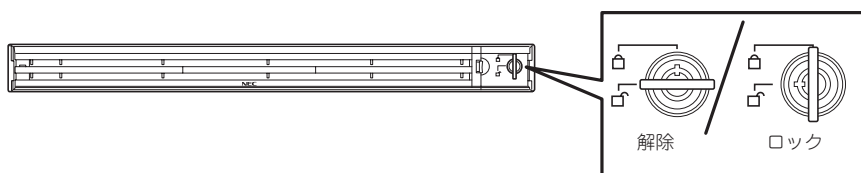
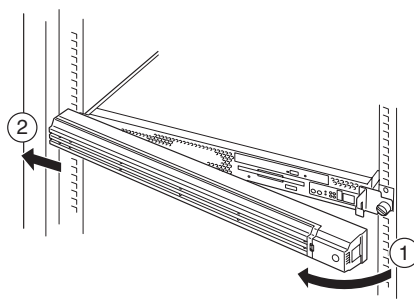
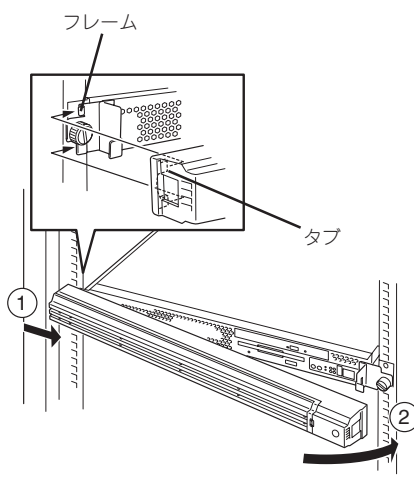
重要 **ラックに搭載している場合は、周辺機器を接続した後ケーブルがラックのドアや側面のガイドレールなどに当たらないようフォーミングしてください。**

基本的な操作

ハードウェアの基本的な操作の方法について説明します。

フロントベゼル

ラックに搭載した本体の電源のON/OFFやフロッピーディスクドライブ、CD-ROMドライブを取り扱うときはフロントベゼルを取り外します(卓上に設置した場合は、フロントベゼルを取り付けることはできません)。

重要 **フロントベゼルは、添付のセキュリティキーでロックを解除しないと開けることができません。**

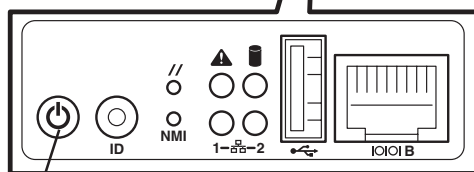
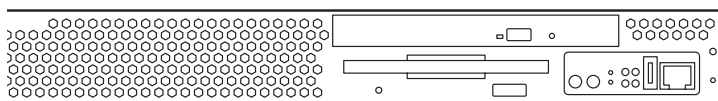
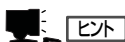
1. キースロットに添付のセキュリティキーを差し込み、キーをフロントベゼル側に軽く押しながら回してロックを解除する。

2. フロントベゼルの右端を軽く持って手前に引く。
3. フロントベゼルを左に少しスライドさせてタブをフレームから外して本体から取り外す。

フロントベゼルを取り付けるときは、フロントベゼルの左端のタブを本体のフレームに引っかけるようにしながら取り付けます。取り付けた後はセキュリティのためにもキーでロックしてください。

POWERスイッチ　- 電源のON/OFF/再起動 -

本体の電源は前面にあるPOWERスイッチを押すとONの状態になります。
次の順序で電源をONにします。

重要

- **添付の「バックアップCD-ROM」をCD-ROMドライブにセットしたまま起動するとシステムを再インストールしてしまいます(このときに確認のメッセージなどは表示されません)。**
- **添付の「EXPRESSBUILDER(SE)」をCD-ROMドライブにセットしたまま起動するとEXPRESSBUILDER(SE)が起動し、通常の運用には利用できません。**

1. ラックに搭載している場合は、フロントベゼルを取り外す。
2. フロッピーディスクドライブにフロッピーディスクをセットしていないことを確認する。
3. 本体前面にあるPOWERスイッチを押す。

   POWERランプが緑色に点灯します。

POWERスイッチ
(POWERランプ兼用)

ヒント

電源コードを接続するとハードウェアの初期診断を始めます(約5秒間)。初期診断中はPOWERスイッチは機能しません。電源コードの接続直後は、約5秒ほど時間をおいてからPOWERスイッチを押してください。

電源ONの後、自己診断プログラム(POST)を実行してハードウェアを診断しています。POSTを完了するとシステムが起動します。システムの起動後はManagement Consoleから本体の設定や管理ができます。4章をご覧ください。

本体の電源のOFFやリセット(再起動)はManagement Consoleを使用します。4章を参照してください。Management Consoleから電源をOFFできないときは本体のPOWERスイッチを4秒以上押し続けてください(強制電源OFF)。

フロッピーディスクドライブ

本体前面にフロッピーディスクを使ったデータの読み出し(リード)・保存(ライト)を行うことのできる3.5インチフロッピーディスクドライブが搭載されています。
3.5インチの2HDフロッピーディスク(1.44Mバイト)と2DDフロッピーディスク(720Kバイト)を使用することができます。

フロッピーディスクのセット/取り出し

フロッピーディスクをフロッピーディスクドライブにセットする前に本体の電源がON(POWERランプ点灯)になっていることを確認してください。
フロッピーディスクをフロッピーディスクドライブに完全に押し込むと「カチッ」と音がして、フロッピーディスクドライブのイジェクトボタンが少し飛び出します。
イジェクトボタンを押すとセットしたフロッピーディスクをフロッピーディスクドライブから取り出せます。

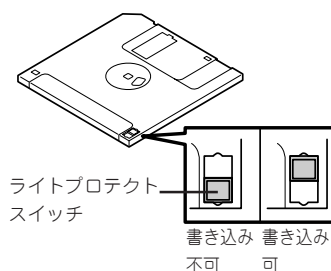
- フォーマット済みのフロッピーディスクを使用してください。
- フロッピーディスクをセットした後に本体の電源をONにしたり、再起動するとフロッピーディスクから起動します。フロッピーディスク内にシステムがないと起動できません。
- フロッピーディスクアクセスランプが消灯していることを確認してからフロッピーディスクを取り出してください。アクセスランプが点灯中に取り出すとデータが破壊されるおそれがあります。

フロッピーディスクの取り扱いについて

フロッピーディスクは、データを保存する大切なものです。またその構造は非常にデリケートにできていますので、次の点に注意して取り扱ってください。

- フロッピーディスクドライブにはていねいに奥まで挿入してください。
- ラベルは正しい位置に貼り付けてください。
- 鉛筆やボールペンで直接フロッピーディスクに書き込んだりしないでください。
- シャッタを開けないでください。
- ゴミやほこりの多いところでは使用しないでください。
- フロッピーディスクの上に物を置かないでください。
- 直射日光の当たる場所や暖房器具の近くなど温度の高くなる場所には置かないでください。
- たばこの煙に当たるところには置かないでください。
- 水などの液体の近くや薬品の近くには置かないでください。
- 磁石など磁気を帯びたものを近づけないでください。

- クリップなどではさんだり、落としたりしないでください。
- 磁気やほこりから保護できる専用の収納ケースに保管してください。
- フロッピーディスクは、保存している内容を誤って消すことのないようにライトプロテクト(書き込み禁止)ができるようになっています。ライトプロテクトされているフロッピーディスクは、読み出しはできますが、ディスクのフォーマットやデータの書き込みができません。重要なデータの入っているフロッピーディスクは、書き込み時以外はライトプロテクトをしておくようお勧めします。3.5インチフロッピーディスクのライトプロテクトは、ディスク裏面のライトプロテクトスイッチで行います。

- フロッピーディスクは、とてもデリケートな記憶媒体です。ほこりや温度変化によってデータが失われることがあります。また、オペレータの操作ミスや装置自身の故障などによってもデータを失う場合があります。このような場合を考えて、万一に備えて大切なデータは定期的にバックアップをとっておくことをお勧めします。(本体に添付されているフロッピーディスクは必ずバックアップをとってください。)

CD-ROMドライブ

本体前面にCD-ROMドライブがあります。CD-ROMドライブはCD-ROM(読み出し専用のコンパクトディスク)のデータを読むための装置です。

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- CD-ROMドライブのトレーを引き出したまま放置しない

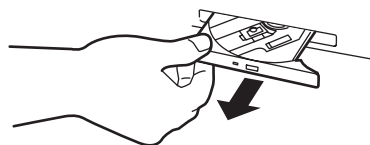
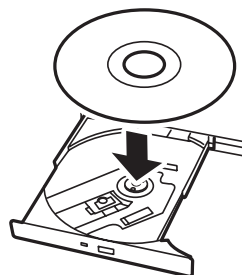
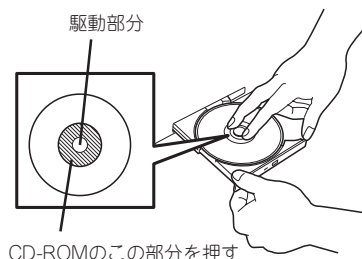
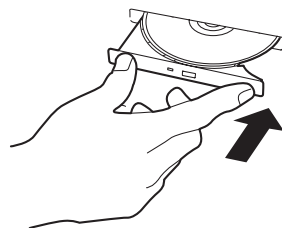
CD-ROMのセット/取り出し

CD-ROMは次の手順でセットします。

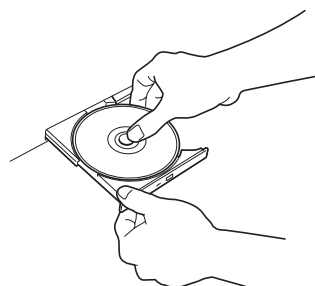
1. CD-ROMをCD-ROMドライブにセットする前に本体の電源がON(POWERランプが緑色に点灯)になっていることを確認する。

2. CD-ROMドライブ前面のCDトレーイジェクトボタンを押す。

   トレーが少し出てきます。

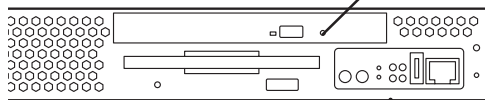
3. トレーを軽く持って手前に引き出し、トレーが止まるまで引き出す。

4. CD-ROMの文字が印刷されている面を上にしてトレーの上に静かに、確実に置く。

5. 右図のように片方の手でトレーを持ちながら、もう一方の手でトレーの中心にある駆動部分にCD-ROMの穴がはまるように指で押して、トレーにセットする。

6. トレーの前面を軽く押して元に戻す。

CD-ROMの取り出しは、CD-ROMをセットするときと同じようにCDトレーイジェクトボタンを押してトレーを引き出します。

アクセスランプが点灯しているときはCDにアクセスしていることを示します。CDトレーイジェクトボタンを押す前にアクセスランプが点灯していないことを確認してください。

右図のように、片方の手でトレーを持ち、もう一方の手でトレーの中心にある駆動部分を押さえながらCD-ROMの端を軽くつまみ上げるようにしてトレーから取り出します。

CD-ROMを取り出したらトレーを元に戻してください。

取り出せなくなったときの方法

CDトレーイジェクトボタンを押してもCD-ROMが取り出せない場合は、次の手順に従ってCD-ROMを取り出します。

1. POWERスイッチを押して本体の電源をOFF（POWERランプ消灯）にする。
2. 直径約1.2mm、長さ約100mmの金属製のピン（太めのゼムクリップを引き伸ばして代用できる）をCD-ROM前面右側にある強制イジェクトホールに差し込んで、トレーが出てくるまでゆっくりと押す。

重要

- **つま楊枝やプラスチックなど折れやすいものを使用しないでください。**
- **上記の手順を行ってもCD-ROMが取り出せない場合は、保守サービス会社に連絡してください。**

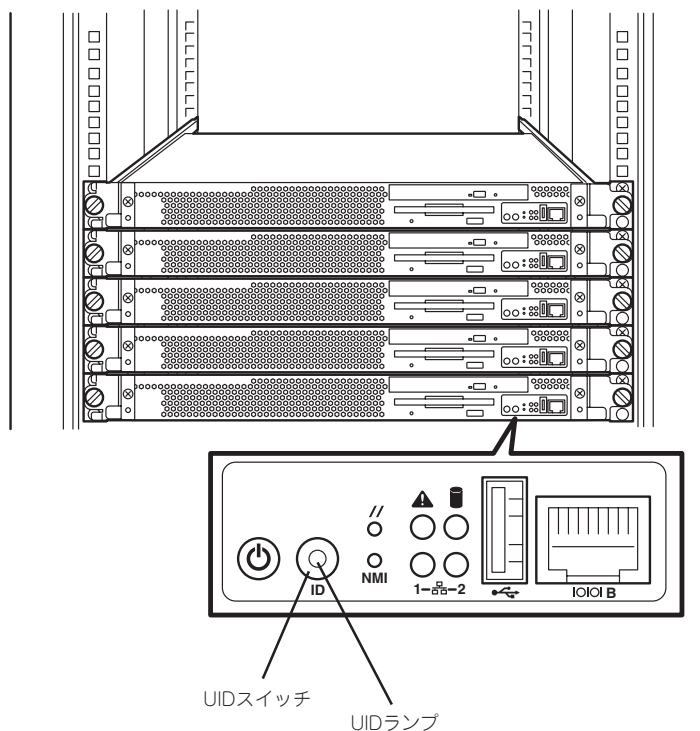
3. トレーを持って引き出す。
4. CD-ROMを取り出す。
5. トレーを押して元に戻す。

CD-ROMの取り扱いについて

使用するCD-ROMは次の点に注意して取り扱ってください。

- CD規格に準拠しない「コピーガード付きCD」などのディスクにつきましては、CD再生機器における再生の保証はいたしかねます。
- CD-ROMを落とさないでください。
- CD-ROMの上にものを置いたり、曲げたりしないでください。
- CD-ROMにラベルなどを貼らないでください。
- 信号面(文字などが印刷されていない面)に手を触れないでください。
- 文字の書かれている面を上にして、トレーにていねいに置いてください。
- キズをつけたり、鉛筆やボールペンで文字などを直接CD-ROMに書き込まないでください。
- たばこの煙の当たるところには置かないでください。
- 直射日光の当たる場所や暖房器具の近くなど温度の高くなる場所には置かないでください。
- 指紋やほこりがついたときは、乾いた柔らかい布で、内側から外側に向けてゆっくり、ていねいにふいてください。
- 清掃の際は、CD専用のクリーナをお使いください。レコード用のスプレー、クリーナ、ベンジン、シンナーなどは使わないでください。
- 使用後は、専用の収納ケースに保管してください。

UIDスイッチ　- 本体の確認 -

複数の機器を1つのラックに搭載している場合、保守をしようとしている装置がどれであるかを見分けるために本体の前面および背面には「UID(ユニットID)ランプ」がもうけられています。

UID(ユニットID)スイッチを押すとUIDランプが点灯します。もう一度押すとランプは消灯します。
ラック背面からの保守は、暗く、狭い中での作業となり、正常に動作している機器の電源やインタフェースケーブルを取り外したりするおそれがあります。UIDスイッチを使って保守する本装置を確認してから作業をすることをお勧めします。

3 システムのセットアップ

購入後、初めて本製品をセットアップする時の手順を説明します。

セットアップの準備

セットアップには、本体以外のマシンや接続のためのケーブルなどが必要となります。また、それぞれのマシンについてもソフトウェアのインストールなどの準備が必要となります。

- **本体**

  購入時のハードディスク上にはファイアウォールのモジュール、および基本設定ツールがインストール済みです。これらを使用して、コンフィグレーションをしてください。

- **管理クライアント**

  システムの基本設定をするために使用する管理コンピュータとして使用します。
  設定ツール(Management Console)にアクセスするためのブラウザがインストールされていることを確認してください。ブラウザにはInternet Explorer 6.0 SP1(日本語版・Windows版)を推奨します。

- **ライセンスキー**

  本製品のセットアップには、ライセンスキーが必要となります。セットアップの前に準備してください。入手方法については、1章の「ライセンスキー」を参照してください。

セットアップ

本製品のセットアップについて順を追って説明します。

設定手順の流れ

設定手順の流れを以下に示します。

1. 初期導入設定用ディスクによる設定

1. 初期導入設定用ディスクの作成
2. 初期導入設定用ディスクによるセットアップ

2. システムの基本設定

3. かんたん設定によるセットアップ

4. バックアップ

1. システム基本情報のバックアップ
2. セキュリティポリシーのバックアップ

5. ESMPRO/ServerAgentのセットアップ

6. マザーボード情報のバックアップ

初期導入設定用ディスクによる設定

初期導入設定用ディスクでの設定方法について説明します。

初期導入設定用ディスクの作成

「初期導入設定用ディスク」はExpress5800/SG300をネットワークに接続するために必要な設定情報を保存したセットアップ用ディスクです。
添付の「初期導入設定用ディスク」にあらかじめ入っている「初期導入設定ツール」を使用して作成します。「初期導入設定ツール」は、Windows 98/NT4.0/2000/XPが動作するコンピュータで動作します。

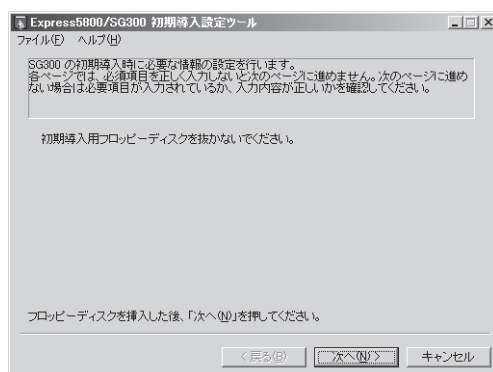
初期導入設定ツールの実行と操作の流れ

次の順序で初期導入設定用ディスクを作成します。それぞれの設定項目については、この後に説明しています。

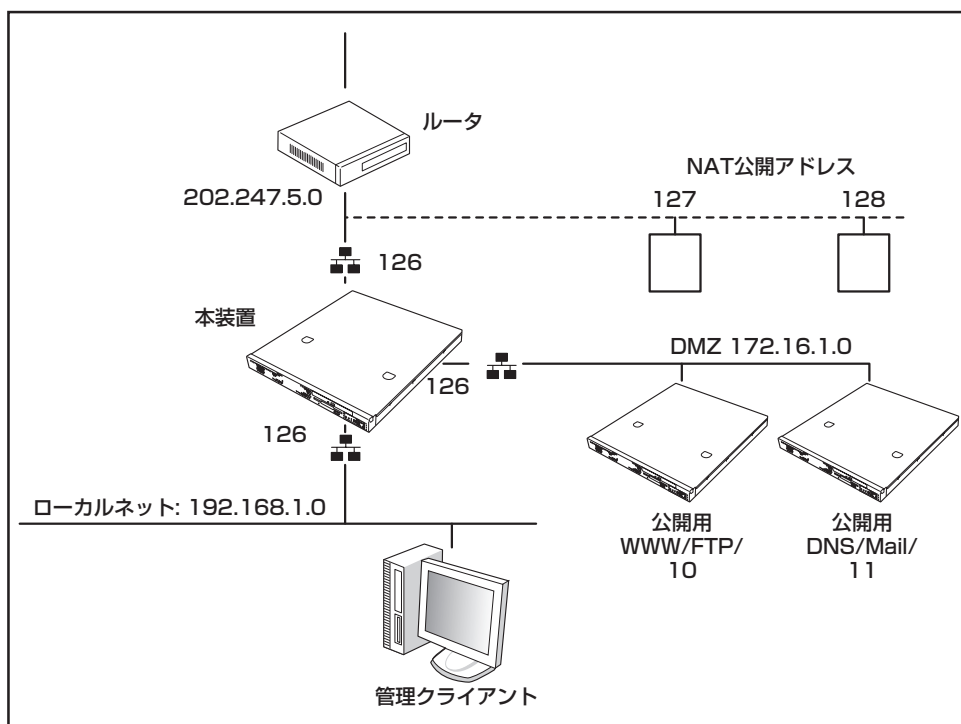
1. 管理クライアントマシンのフロッピーディスクドライブに添付の「初期導入設定用ディスク」をセットする。
2. フロッピーディスクドライブ内の「初期導入設定ツール(StartupConf.exe)」を実行する。

   「初期導入設定ツール」が起動します。
3. 開始画面が表示されたら[次へ]をクリックし、設定の入力を開始する。

   プログラムは、ウィザード形式となっており、各ページで設定に必要事項を入力して進んでいきます。必須項目が入力されていない場合や入力情報に誤りがある場合は警告メッセージが表示されますので、項目を正しく入力し直してください。入力事項の詳細については、後述の説明を参照してください。すべての項目の入力が完了すると、フロッピーディスクに設定情報を書き込んで終了します。
4. 初期導入設定用ディスクをフロッピーディスクドライブから取り出し、「初期導入設定用ディスクによるセットアップ」に進む。

重要

初期導入設定用ディスクは再セットアップの際にも使用します。大切に保管してください。

入力項目の設定

以下のネットワーク構成を例にして「初期導入設定ツール」で入力する項目について説明します。

設定項目表

初期導入設定用ディスクを作成する際に必要となる項目の一覧です。前ページのネットワーク構成例を元に本手順で設定する内容を設定例欄に記入してあります。

実際に使用されるネットワーク環境に即した内容を、該当する項目のお客様記入欄に記入し、以降の手順でExpress5800/SG300本体を設定する際に参照してください。

設定項目	詳細設定項目		設定例	お客様記入欄
ネットワークインタフェースの設定①	ホスト名		firewall.nec.co.jp	
	内側ネットワーク	IPアドレス	192.168.1.126	
		ネットマスク	255.255.255.0	
	外側ネットワーク	IPアドレス	202.247.5.126	
		ネットマスク	255.255.255.0	
ネットワークインタフェースの設定②	DMZ	IPアドレス	172.16.1.126	
		ネットマスク	255.255.255.0	
	予備ネットワーク	IPアドレス		
		ネットマスク		
ルーティングの設定	デフォルトゲートウェイ	IPアドレス	202.247.5.254	
	静的ルーティング	IPアドレス		
		ネットマスク		
		ゲートウェイ		
ネームサーバ NTPサーバ の設定	ネームサーバ 1	IPアドレス		
	ネームサーバ 2	IPアドレス		
	NTPサーバ	IPアドレス		
リモートメンテナンス機能の設定	管理者のメールアドレス		admin@nec.co.jp	
	メールゲートウェイ	IPアドレス		
	TRAP送信先ホスト	IPアドレス		
Management Console の設定	ポート番号		18000	
	管理者アカウント		admin	
	パスワード			
	パスワード（確認用）			

設定項目	詳細設定項目	設定例	お客様記入欄
SSHに関する設定	Secure Shell (SSH)を使用する	オン	
	ポート番号	18022	
	管理者アカウント	admin	
	パスワード		
	パスワード (確認用)		
管理クライアントの設定	接続元1 IPアドレス	192.168.1.10	
	接続元2 IPアドレス		
	接続元3 IPアドレス		
	接続元4 IPアドレス		
二重化のセットアップ	二重化構成で使用する	オフ	
キーの入力	ライセンスキー1		
	ライセンスキー2		
	サポートキー1		
	サポートキー2		

● **ネットワークインタフェースの設定**

Express5800/SG300のネットワークの設定をします。

— ホスト名(必須項目)

ホスト名はドメイン名まで含めたFQDNの形式で入力してください。

— 内側IPアドレス(必須項目)

内側IPアドレスを入力します。

— 内側ネットマスク(必須項目)

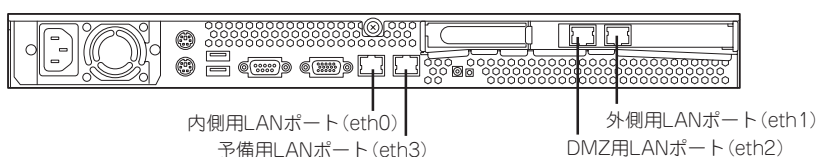
内側IPアドレスに対するサブネットマスクを入力します。

— 外側IPアドレス(必須項目)

外側IPアドレスを入力します。

— 外側ネットマスク(必須項目)

外側IPアドレスに対するサブネットマスクを入力します。

各ネットワークインタフェースが、本装置のどのLANポートに相当しているかを下図に示します。

● **ネットワークインタフェースの設定**

非武装地帯(DMZ)を構成するネットワークと予備ネットワークの設定をします。

— DMZ IPアドレス

DMZ用IPアドレスを入力します。

— DMZネットマスク

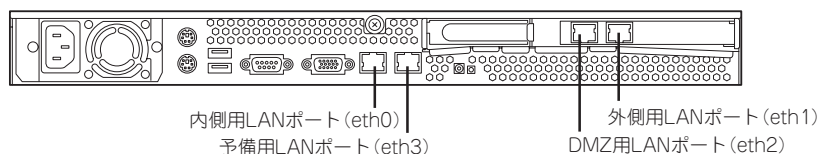
DMZ用IPアドレスに対するサブネットマスクを入力します。

— 予備IPアドレス

予備として用意されている本装置の4番目のネットワークポートのIPアドレスを入力します。内部ネットワークでもうひとつのセグメントを用意する場合や、二重化構成時にサーバ間監視専用インタフェース(ハートビート)として使用します。

— 予備ネットマスク

予備IPアドレスに対するサブネットマスクを入力します。

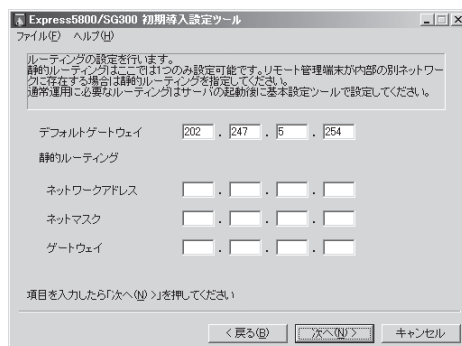
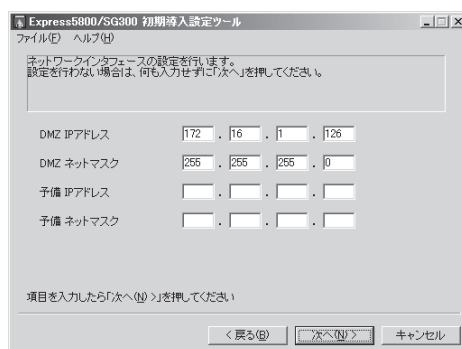
各ネットワークインタフェースが、本装置のどのLANポートに相当しているかを下図に示します。

● **ルーティングの設定**

ルーティングの設定をします。静的ルーティングはここでは1つのみ設定可能です。リモート管理端末が内部の別ネットワークに存在する場合は静的ルーティングを指定してください。通常、運用に必要なルーティングはExpress5800/SG300の起動後にManagement Consoleから設定してください。

— デフォルトゲートウェイ(必須項目)

デフォルトゲートウェイのIPアドレスを設定します。

— 静的ルーティング

宛先ネットワークアドレスとネットマスクおよびゲートウェイの組み合わせを指定します。

● **ネームサーバ/NTPサーバの設定**

ネームサーバ/NTPサーバの設定をします。

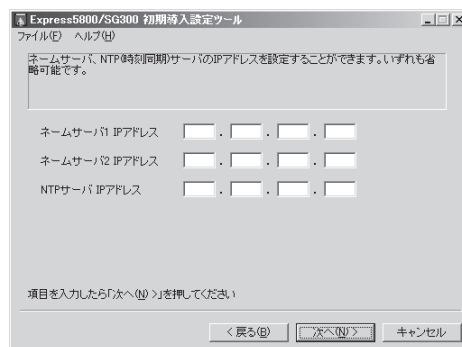
— ネームサーバ1 IPアドレス

ネームサーバ1のIPアドレスを入力します。

— ネームサーバ2 IPアドレス

ネームサーバ2のIPアドレスを入力します。

— NTPサーバIPアドレス

NTPサーバのIPアドレスを入力します。

● **リモートメンテナンス機能の設定**

メールアドレスとリモートメンテナンス機能の利用に関する設定をします。

— 管理者のメールアドレス(必須項目)

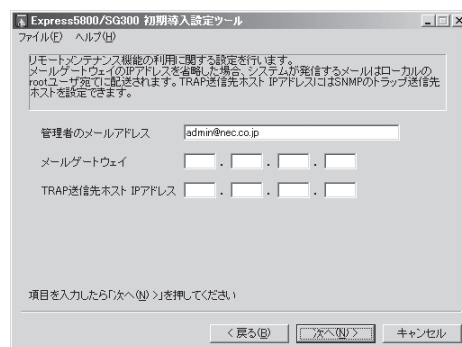
管理者のメールアドレスを指定します。

— メールゲートウェイの設定

メールゲートウェイのIPアドレスを入力します。

メールゲートウェイのIPアドレスを省略した場合、システムが発信するメールはローカルのrootユーザ宛てに配送されます。

— TRAP送信先ホストIPアドレスの設定

SNMPのTRAP送信先ホストを設定します。

- **Management Consoleに関する設定**

  Management Consoleに関する設定をします。

  — ポート番号(必須項目)

  Management Consoleで使用するポート番号を入力します。規定値は、18000です。必要に応じて変更してください。

  — 管理者アカウント名(必須項目)

  管理クライアントからManagement Consoleに接続する際の管理者名(15文字以内)を入力します。

  — パスワード(必須項目)

  管理者に対する、パスワードを設定します。

  — パスワードの再入力(必須項目)

  確認のため、パスワードを再度入力します。

- **SSHに関する設定**

  SSHに関する設定をします。

  — Secure Shell(SSH)を使用する

  使用する場合:
  　チェックボックスをチェック
  使用しない場合:
  　チェックボックスのチェックをはずす。

  — ポート番号

  SSHで使用するポート番号を入力します。既定値は18022です。必要に応じて変更してください。

  — 管理者アカウント名

  管理クライアントからSSHで接続する際の管理者名(15文字以内)を入力します。

  — パスワード

  管理者に対する、パスワードを設定します。

  — パスワードの再入力

  確認のため、パスワードを再度入力します。

● **管理クライアントの設定**

Express5800/SG300が接続を許可する管理クライアントのIPアドレスを登録します。

[接続元1 IPアドレス]は入力必須の項目です。残りのIPアドレスは必要に応じて登録してください。

接続元のIPアドレスは、Management Consoleから追加登録することができます。Management Consoleにログイン後、[Management Console]→[リモートメンテナンス]の順に進むと設定画面が表示されます。

● **二重化のセットアップ**

2台のExpress5800/SG300を使用して可用性を高めることができます。二重化を構築する場合は、[設定対象ホストを二重化構成で使用する]にチェックしてください。二重化構成の詳細については、この章の「二重化構成について」で説明しています。

二重化構成で使用する場合、相手となるExpress5800/SG300の初期導入用設定ディスクの作成の際にもチェックを入れておくことをお勧めします(ただし、二重化の設定は後からでもできます)。

● **ライセンスの設定**

Express5800/SG300をファイアウォールとして使用するために、この画面で入手しているライセンスキーを入力してください。

また、ソフトウェアサポートサービスの契約をしている場合は、発行されたサポートキーを併せて入力します。

ライセンスキー、およびサポートキーの詳細については、1章の「ライセンスキー」、および「ソフトウェアサポート」を参照してください。

ライセンスキー、およびサポートキーは、初期導入設定用ディスクによる設定の後、Management Consoleからも登録することができます。Management Consoleにログイン後、[ファイアウォール]→[ライセンス確認/登録]の順に進むと登録画面が表示されます。

初期導入設定用ディスクによるセットアップ

初期導入設定ツールで作成した「初期導入設定用ディスク」を使用してセットアップし、管理クライアントをExpress5800/SG300へ接続します。

セットアップ手順

以下の手順でセットアップします。
正しくセットアップできないときは、この後の「セットアップに失敗した場合」を参照してください。

1. Express5800/SG300の電源がOFFの状態で、管理クライアントとExpress5800/SG300背面にあるLANポートインタフェース（内部ネットワーク用）をクロスケーブルで接続するか、Express5800/SG300が接続されている内部ネットワークのハブなどに管理クライアントのLANケーブルを接続する。

2. 初期導入設定用ディスクをExpress5800/SG300のフロッピーディスクドライブにセットする。

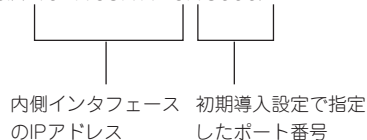
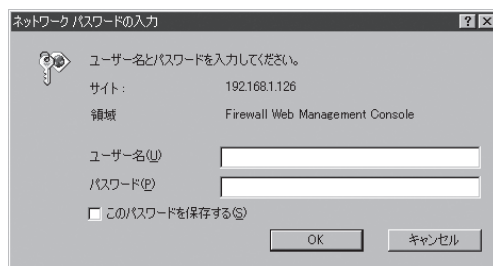
3. 本体のPOWERスイッチを押し、POWERランプが点灯することを確認する。

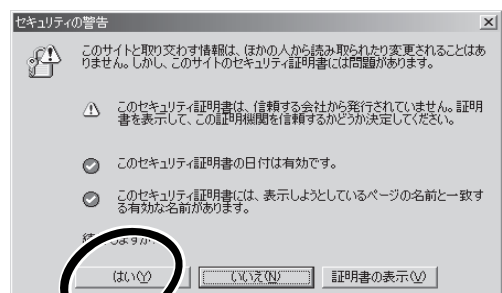
   しばらくすると、初期導入設定用ディスクから設定情報を読み取り、自動的にセットアップを進めます。2～3分ほどでセットアップが完了します。

4. 管理クライアントのブラウザを使用して、Express5800/SG300のManagement Consoleへ接続する。

   重要

   Management Consoleには必ず内部ネットワークの管理クライアントから接続するようにしてください。外部から接続を許可する設定には絶対にしないでください。また、Management Consoleを使用する場合は、Internet Explorer 6.0 SP1（日本語版・Windows版）以上を使用してください。

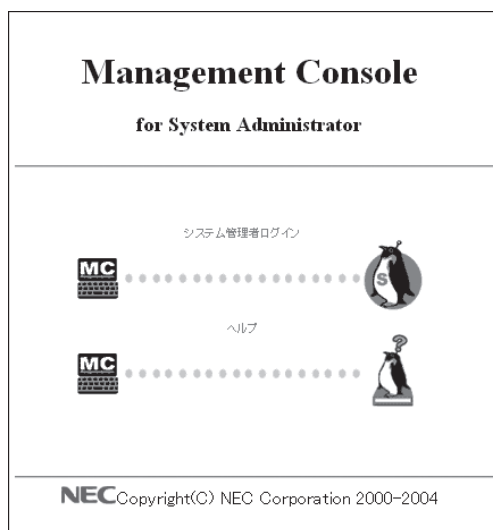
   このときのURLには、Express5800/SG300の内側（管理クライアントが設置されているネットワーク側）のインタフェースのIPアドレスと初期導入設定ツールで設定したポート番号を指定します。

   接続すると、セキュリティの警告が表示されます。

5. ［はい］をクリックする。

6. 初期導入設定ツールで設定した管理者アカウント名とパスワードを入力する。

接続に成功すると、Management Consoleのログイン画面が表示されます。

7. [システム管理者ログイン]をクリックする。

Management Consoleのトップ画面が表示されます。

システムのセットアップ

8. 左側のメニューの[基本設定]アイコンをクリックする。

初期導入設定ツールで設定した内容が正しく表示されていることを確認してください。

これで初期導入設定用ディスクによるセットアップ、管理クライアントの接続は完了です。以降の説明では、管理クライアントからの操作でシステムのセットアップを行います。

セットアップの完了が確認できたらセットした初期導入設定用ディスクをフロッピーディスクドライブから取り出して大切に保管してください。再セットアップの時に使用することができます。

上記の画面上で設定を変更することができますが、変更する前に後述の「システムの基本設定」の説明をよくお読みください。この画面で設定項目とその説明があります。

セットアップに失敗した場合

システムのセットアップに失敗した場合は、自動的に電源がOFF（POWERランプ消灯）になり、ユーザーに異常終了したことを知らせます。正常にセットアップを完了できなかった場合は、初期導入設定用ディスクに書き出されるログファイル「logging.txt」の内容を確認し、再度初期導入設定ツールを使用して初期導入設定用ディスクを作成してください。

〈主なログの出力例〉

「Error: cannot open: /mnt/floppy/fwsinit.ini」

→ 初期導入設定用ディスク中の設定に誤りがある場合に表示されます。

「Error: bad user name (WbMC)」

→ 初期導入設定用ディスク中のManagement Consoleの管理者名の指定に誤りがある場合に表示されます。

「Error: bad user name (SSH)」

→ 初期導入設定用ディスク中のSSHの管理者名の指定に誤りがある場合に表示されます。

「Error: port number of WbMC and SSH is the same.」

→ Management Consoleのポート番号とSSHのポート番号に同一の値が設定された場合に表示されます。Management Consoleのポート番号とSSHのポート番号には違う値を設定する必要があります。

「Error: fwsetup failure.」

→ ファイアウォールへ初期導入設定ができない場合に表示されます。初期導入設定用ディスクの設定に誤りがあります。

初期導入設定用ディスクの内容が誤っていた場合、初期導入設定用ディスクの設定内容を修正して再度セットアップすることができます。
ただし、以下の操作を行った場合には、初期導入設定用ディスクによる設定の機能はOFFになります。設定の変更が、基本設定ツール(sgsetup)もしくはManagement Consoleからしかできなくなりますので注意してください。

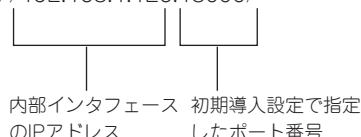
- Management Consoleの基本設定画面から[設定]をクリックした場合。
- コンソールから基本設定ツール(sgsetup)を実行した場合。

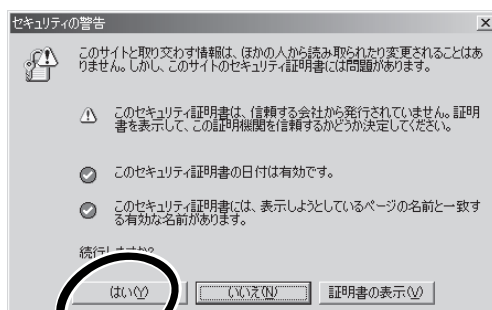
システムの基本設定

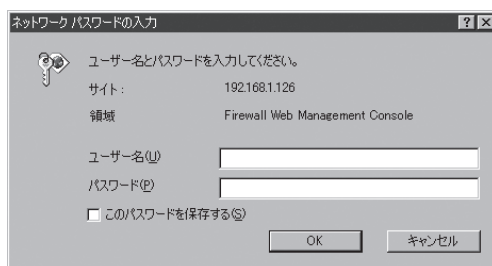
前述の「初期導入設定用ディスクによる設定」で管理クライアントからExpress5800/SG300に接続するための最低限必要なセットアップが完了しました。ここからは、Management Consoleを使用して、さらに詳細なセットアップを行います。
以下にManagement Consoleを使用した基本設定の項目や実際の手順の流れを示します。

重要 **Management Consoleには必ず内部ネットワークの管理クライアントから接続するようにしてください。外部から接続を許可する設定には絶対にしないでください。また、Management Consoleを使用する場合は、Internet Explorer 6.0 SP1(日本語版・Windows版)以上を使用してください。**

1. 管理クライアントのウェブブラウザを使用して、Express5800/SG300のManagement Consoleに接続する。

   このときのURLには、Express5800/SG300の内側(管理クライアントが設置されているネットワーク側)のインタフェースのIPアドレスと初期導入設定ツールで設定したポート番号を指定します。

   接続すると、セキュリティの警告が表示されます。

2. [はい]をクリックする。

3. 初期導入設定ツールで設定した管理者アカウント名とパスワードを入力する。

   接続に成功すると、Management Consoleのトップメニューの画面が表示されます。

4. 左側のメニューから[基本設定]アイコンをクリックする。

基本設定画面が表示されます。

5. 次の基本設定項目を設定する。

Express5800/SG300のホスト名、IPアドレス、ルーティングなどの初期導入設定用ディスクで設定した項目については、設定値を確認してください。

ヒント

- [ホスト名]と[インタフェース]、[デフォルトゲートウェイ]の項目の背景色が他と異なるのは、これらの項目を変更すると装置の再起動が必要となることを示しています。その他の項目は設定を変更しても、再起動をする必要はありません。
- 変更や追加した内容を破棄したい場合は、[元に戻す]をクリックして終了してください。

- ホスト名(FQDN)(必須項目)

  ホスト名を入力します。

- インタフェース(IPアドレス/ネットマスク/MTU値)(必須項目)

  各インタフェースのIPアドレス、ネットマスクおよびMTU値を入力します。各インタフェースが、本装置のどのLANポートに相当するかは52ページを参照してください。

- ネームサーバ

  ネームサーバのIPアドレスを入力します。(複数入力可)

- 管理者メールアドレス(必須項目)

  管理者のメールアドレスを指定します。

- メールゲートウェイ

  使用か未使用かを指定します。使用の場合は、メールゲートウェイのIPアドレスを入力します。

- デフォルトゲートウェイ(必須項目)

  デフォルトゲートウェイのIPアドレスを設定します。

- 静的ルーティング(アドレス/ネットマスク/ゲートウェイ)

  宛先ネットワークアドレスとネットマスクおよびゲートウェイの組み合わせを指定します。必要に応じてインタフェースを「自動」以外に変更し、関連付けたいインタフェースを指定します。

- トラップ送信先ホストのIPアドレス

  SNMPのTRAP送信先ホストを設定します。

- NTP時刻同期サーバ

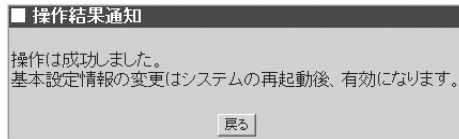
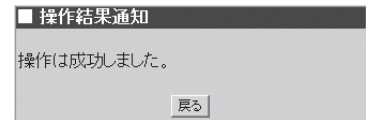
  NTPサーバのIPアドレスを入力します。

- 二重化機能

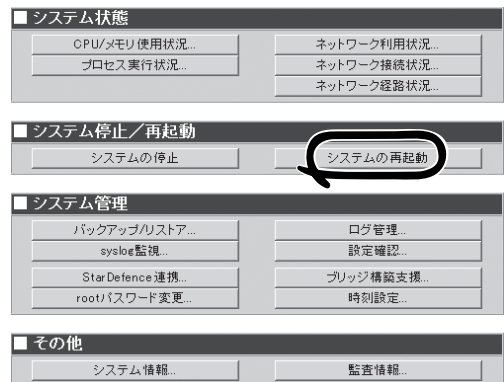
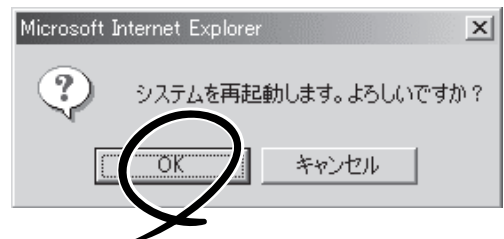
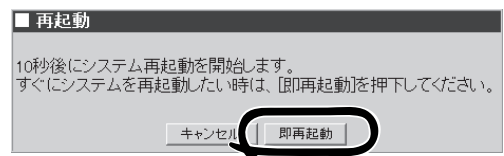
  設定対象のホストを二重化構成で使用する場合は、〔使用〕を選択します。

6. 確認ができたら、[設定]をクリックする。

   操作結果画面が表示されます。

   操作結果画面は、設定内容がシステムの再起動後に有効になる場合と再起動を必要とせずに有効となる場合でメッセージが異なります。
   再起動を促す指示を含むメッセージが表示された場合は、手順7以降を参照して作業を続けてください。再起動の指示が含まれていない場合は、以上で基本設定は完了です。

再起動が必要

再起動は必要なし

7. [戻る]をクリックする。

8. 左側のメニューの[システム]アイコンをクリックし、[システムの再起動]をクリックする。

9. [OK]をクリックする。

10. [即再起動]をクリックし、再起動する。

これでシステムの基本設定は完了です。

セキュリティポリシーのセットアップ

次にネットワークを攻撃から守るための通信制御(以降、「セキュリティポリシー」と呼びます)を設定します。

かんたん設定ウィザードを実行すると、Express5800/SG300を導入するネットワーク環境に即した一般的なセキュリティポリシーを設定することができます。
Management Consoleの「ファイアウォール」メニューから[かんたん設定]をクリックして、Express5800/SG300を導入するネットワーク環境に合わせて、以下の各項で説明する内容を入力、または選択することにより、環境に即したセキュリティポリシーの設定ができます。

セキュリティポリシーの詳細な設定方法については、4章を参照してください。

公開サーバ設定項目表

かんたん設定ウィザードで設定する項目の一覧です。49ページのネットワーク構成例を元にここでの手順で設定する内容を設定例欄に記入しています。

実際に使用されるネットワーク環境に即した内容を、該当する項目のお客様記入欄に記入し、以降の手順でExpress5800/SG300本体を設定する際に参照してください。

設定項目		詳細設定項目	設定例	お客様記入欄
DMZ		あり/なし	あり	
アドレス変換		する/しない	する	
HTTPサーバ	1	公開IPアドレス	202.247.5.127	
		内部IPアドレス	172.16.1.10	
		ポート番号	80	
	2	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
	3	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
ウェブサーバ		公開IPアドレス	202.247.5.127	
		内部IPアドレス	172.16.1.10	
メールサーバ		公開IPアドレス	202.247.5.128	
		内部IPアドレス	172.16.1.11	
ファイルサーバ		公開IPアドレス	202.247.5.127	
		内部IPアドレス	172.16.1.10	

設定項目		詳細設定項目	設定例	お客様記入欄
ネームサーバ		公開IPアドレス	202.247.5.128	
		内部IPアドレス	172.16.1.11	
その他のサーバ	1	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
	2	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
	3	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
	4	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
	5	公開IPアドレス		
		内部IPアドレス		
		ポート番号		
内部からの利用を許可するサービス		ウェブサービス(HTTP/HTTPS)	許可する	
		メールサービス(SMTP)	許可する	
		ファイル転送サービス(FTP)	許可する	
		ネームサービス(DNS)	許可する	
		時刻同期サービス(NTP)	許可しない	
不正アクセス対策		レベル	ベーシック	
ユーザ認証		する/しない	しない	
		ポート番号		

Management Consoleの起動

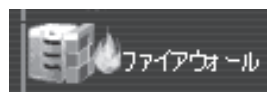
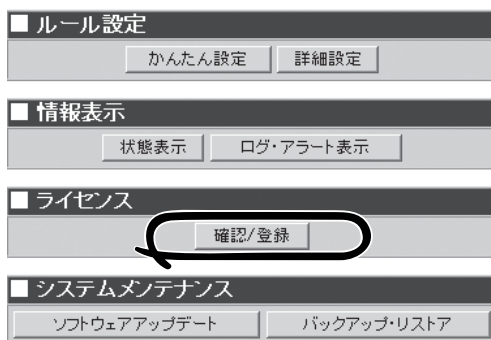
Express5800/SG300の内部ネットワークと接続している管理クライアントでウェブブラウザを起動し、Management Consoleに接続します(Management Consoleの接続については、前述の「システムの基本設定」を参照してください)。

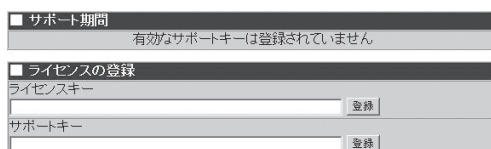
ライセンスとソフトウェアサポートサービスの登録

ライセンスの登録を行います。すでに初期導入設定用ディスクによる設定でライセンスの登録を完了している場合は、本項目でのライセンス登録は必要ありません。かんたん設定ウィザードによるポリシールールの作成に進んでください。

重要 **ライセンスの登録をしていないと、Express5800/SG300は初期導入設定ディスクや基本設定で登録した内容のみが設定された装置にとしてしか使えません。ファイアウォールのサービスを提供することができません。**

ライセンスキー、サポートキーの取得については1章の「ライセンスキー」および「ソフトウェアサポートサービス」を参照してください。

1. Management Consoleの画面左側に並ぶメニューアイコンから[ファイアフォール]アイコンをクリックする。

2. 「ファイアウォール」メニューでライセンスの[確認/登録]をクリックする。

3. ライセンスキーを入力し、[登録]をクリックする。

   ライセンスの登録完了画面が表示されます。

新たにサポートライセンスを取得する場合は、ライセンスキーの情報が必要となります。
現在有効なキーは、以下のボタンを押すと確認できます。

有効なキーの表示

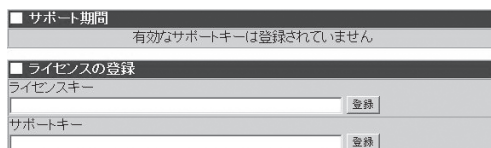
4. [ライセンス登録に戻る]をクリックする。

ライセンスキーを登録しました。

ライセンス登録に戻る

5. <ソフトウェアサポートサービスを購入している場合>

   サポートキーを入力し、[登録]をクリックする。

サポート期間
有効なサポートキーは登録されていません
ライセンスの登録
ライセンスキー
登録
サポートキー
登録

新たにサポートライセンスを取得する場合は、ライセンスキーの情報が必要となります。
現在有効なキーは、以下のボタンを押すと確認できます。

有効なキーの表示

   登録完了画面が表示されます。

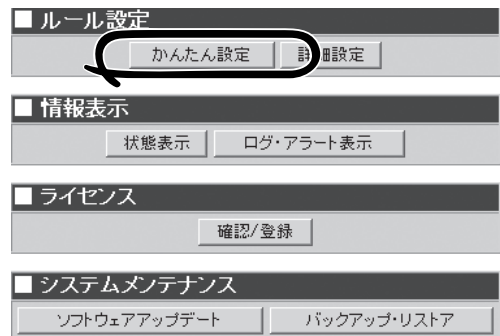
2003年04月01日～2004年03月31日のサポートキーが有効となりました。

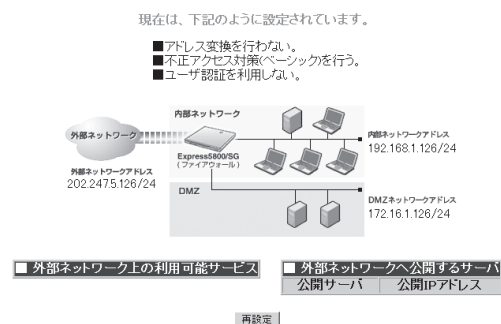
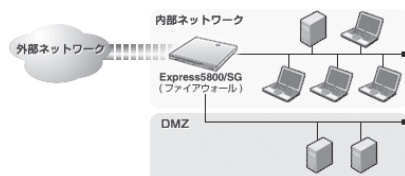
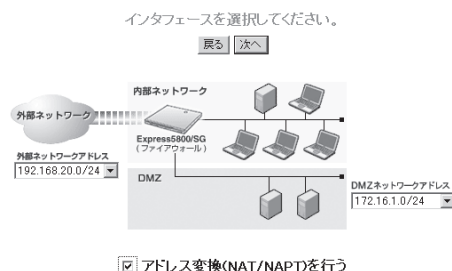
ライセンス登録に戻る

かんたん設定ウィザードによるポリシールールの作成

以下の各手順で入力する値には、63ページの公開サーバ設定項目表に記入したお客様記入欄の対応する項目の値を入力してください。

1. Management Consoleの画面左側に並ぶメニューアイコンから[ファイアフォール]アイコンをクリックする。

2. 「ファイアウォール」メニュー画面が表示されたら、[かんたん設定]をクリックし、かんたん設定ウィザードを実行する。

3. かんたん設定ウィザードを用いて設定した現在の設定内容を通知する設定内容確認画面が表示されたら、[再設定]をクリックする。

   インストール直後など、一度もかんたん設定ウィザードを利用したことがない場合には、設定内容確認画面は表示されず、次のネットワーク構成の選択に移ります。

4. 「DMZあり」にチェックをし、[次へ]をクリックする。

5. 各ネットワークアドレスを設定（本手順では「アドレス変換(NAT/NAPT)を行う」をチェック）して、［次へ］をクリックする。

6. 「公開するウェブサーバ(HTTP)はある」にチェックし、「公開IPアドレス」にウェブサーバとして公開するIPアドレス、「内部IPアドレス」にウェブサーバの実IPアドレスを記入して、［次へ］をクリックする。

7. 「公開するメールサーバ(SMTP)はある」にチェックし、「公開IPアドレス」にメールサーバとして公開するIPアドレス、「内部IPアドレス」にメールサーバの実IPアドレスを記入して、［次へ］をクリックする。

8. 「公開するファイル転送サーバ(FTP)はある」にチェックし、「公開IPアドレス」にファイル転送サーバとして公開するIPアドレス、「内部IPアドレス」にファイル転送サーバの実IPアドレスを記入して、［次へ］をクリックする。

9. 「公開するネームサーバ(DNS)サーバはある」にチェックし、「公開IPアドレス」にネームサーバとして公開するIPアドレス、「内部IPアドレス」にネームサーバの実IPアドレスを記入して、［次へ］をクリックする。

10. 外部へ公開するその他のサーバを設定（本手順では「その他の公開するサーバはない」を選択）して、［次へ］をクリックする。

11. 使用環境に合わせて利用するサービスを「利用する」に変更して、［次へ］をクリックする。

外部ネットワークに公開されている、どのようなサービスを利用しますか？

戻る 次へ

■ 利用するサービス	
ウェブサービス(HTTP/HTTPS)	◉利用する ○利用しない
メールサービス(SMTP)	◉利用する ○利用しない
ファイル転送サービス(FTP)	◉利用する ○利用しない
ネームサービス(DNS)	◉利用する ○利用しない
時刻同期サービス(NTP)	○利用する ◉利用しない

12. 不正アクセス対策レベルを指定(本手順では「ベーシック」を指定)して[次へ]をクリックする。

不正アクセス対策レベルを選択します。

戻る　次へ

◉ ベーシック

○ アドバンス(ベーシックを含む)

○ 上記の対策を行わない(問題がなければ選択しないでください)

13. ユーザ認証に関する設定をして(本手順では「ユーザ認証を利用しない」を選択)、[次へ]をクリックする。

ユーザ認証を利用しますか？

戻る　次へ

◉ ユーザ認証を利用しない

○ ユーザ認証を利用する

ユーザ認証ウェブのポート番号を 18080 とする
(分からない場合は、変更しないで下さい)

どこからの認証を許可しますか？
◉ 内部ネットワークからのみ許可する
○ すべてのネットワークから許可する

14. これまでの手順で設定した内容が正しく反映されていることを確認し、[設定]をクリックする。

設定内容に誤りがある場合は[やり直し]をクリックし、再度設定を行ってください。

下記のように設定してよろしいですか？

■アドレス変換を行う。
■不正アクセス対策(ベーシック)を行う。
■ユーザ認証を利用しない。

■ 外部ネットワーク上の利用可能サービス
ウェブサービス(HTTP/HTTPS)
メールサービス(SMTP)
ファイル転送サービス(FTP)
ネームサービス(DNS)

公開サーバ	公開IPアドレス	内部IPアドレス
ウェブサーバ(HTTP)	202.247.5.127	172.16.1.10:80
メールサーバ(SMTP)	202.247.5.128	172.16.1.11
ファイル転送サーバ(FTP)	202.247.5.127	172.16.1.10
ネームサーバ(DNS)	202.247.5.128	172.16.1.11

■ 外部ネットワークへ公開するサーバ

戻る　やり直し　設定

Express5800/SG300に設定内容が反映され、設定内容の画面が表示されます。

下記のように設定しました。

■アドレス変換を行う。
■不正アクセス対策(ベーシック)を行う。
■ユーザ認証を利用しない。

■ 外部ネットワーク上の利用可能サービス
ウェブサービス(HTTP/HTTPS)
メールサービス(SMTP)
ファイル転送サービス(FTP)
ネームサービス(DNS)

■ 外部ネットワークへ公開するサーバ

公開サーバ	公開IPアドレス	内部IPアドレス
ウェブサーバ(HTTP)	202.247.5.127	172.16.1.10:80
メールサーバ(SMTP)	202.247.5.128	172.16.1.11
ファイル転送サーバ(FTP)	202.247.5.127	172.16.1.10
ネームサーバ(DNS)	202.247.5.128	172.16.1.11

かんたん設定を終了

バックアップ

システムのセットアップが終了した後、万一の故障による再セットアップに備えて、設定した情報のバックアップを作成します。

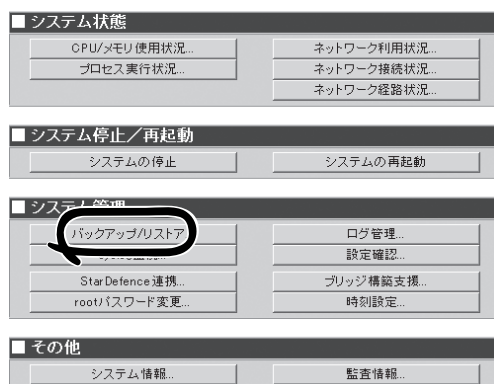
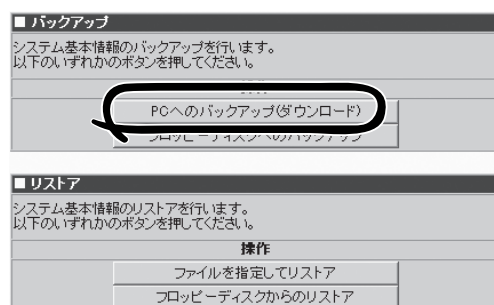
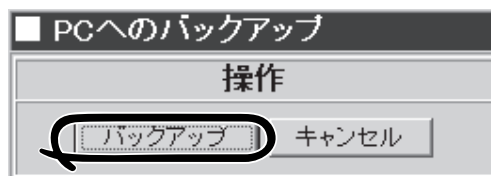
システム基本情報のバックアップ

Management Consoleを使って、システム基本情報をバックアップすることをお勧めします。
システム基本情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧(リストア)できなくなります。次の手順に従ってバックアップをしてください。

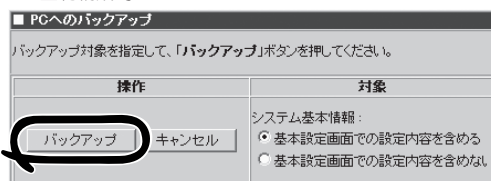
重要 **Management Consoleから操作し、バックアップを行います。Management Consoleへの接続については、4章を参照してください。**

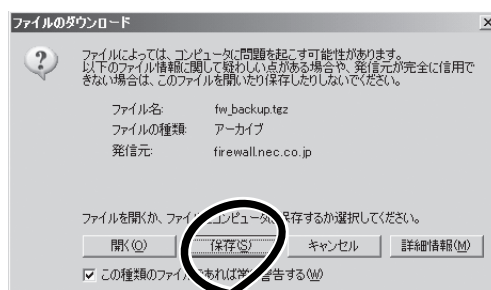
システム基本情報は、管理クライアントへバックアップデータを保存します。

1. 管理クライアントのウェブブラウザを使用してExpress5800/SG300のManagement Consoleに接続し、左側のメニューから[システム]アイコンをクリックする。

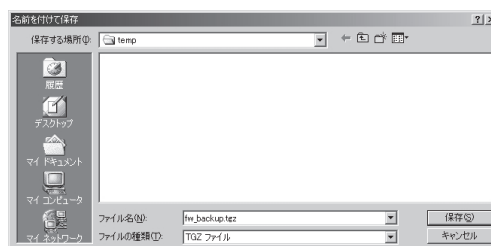
2. [バックアップ/リストア]をクリックする。

3. バックアップ先を選択して、ボタンをクリックする。

4. ［バックアップ］をクリックする。

二重化構成時（基本設定画面で二重化機能を［使用］するに設定した場合）は、バックアップ対象として［基本設定画面での設定内容を含める］を選択して、［バックアップ］をクリックしてください。

なお、運用系から待機系に設定を同期させるためのバックアップの場合は、［基本設定画面での設定内容を含めない］を選択して、［バックアップ］をクリックしてください。

<二重化構成時>

❷［バックアップ］をクリック　❶ バックアップ対象を選択

5. ［保存］をクリックし、保存先を確認して、保存する。

6. 保存するディレクトリを選択し、ファイル名を入力して、［保存］をクリックする。

重要

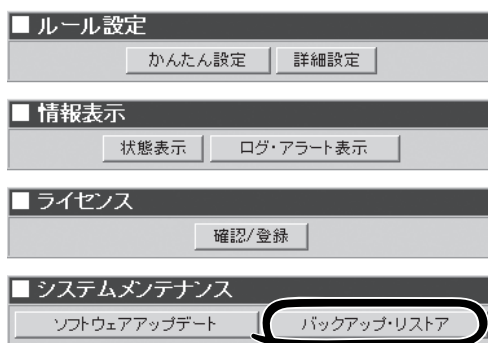
保存したバックアップファイルは、再セットアップ時に使用しますので、大切に保管してください。

セキュリティポリシーのバックアップ

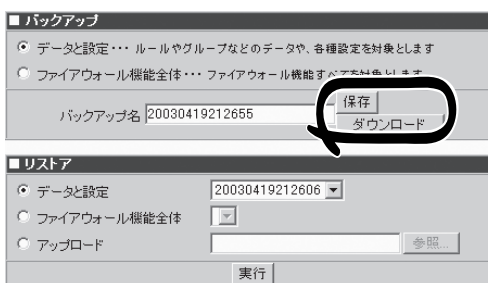
設定したセキュリティポリシーのバックアップを作成します。

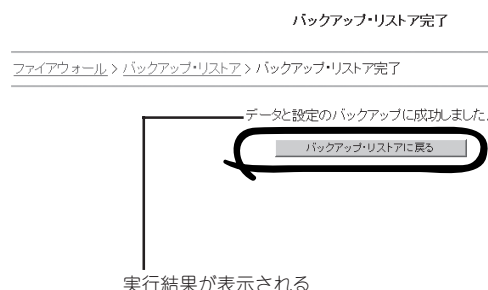
Management Consoleから操作しバックアップを行います。Management Consoleへの接続については、4章を参照してください。

1. 画面左側に並ぶメニューアイコンから[ファイアフォール]アイコンをクリックする。

2. [バックアップ・リストア]をクリックする。

   バックアップ・リストア画面が表示されます。

3. バックアップする内容を選択し、バックアップを実行する。

   Express5800/SG300本体へバックアップする場合には、[保存]を、管理クライアントへバックアップする場合には[ダウンロード]をクリックしてください。

   Express5800/SG300本体へバックアップした場合は、しばらくすると、バックアップ・リストアの完了画面が表示されます。

4. 実行結果を確認後、[バックアップ・リストアに戻る]をクリックする。

ESMPRO/ServerAgentのセットアップ

ESMPRO/ServerAgentは出荷時にインストール済みですが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro.sa/doc

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(5章参照)がインストール済みです。ご利用には別途契約が必要となります。詳しくはお買い求めの販売店または保守サービス会社にお問い合わせください。

シリアル接続の管理PCから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
# export LANG=C
```

マザーボード情報のバックアップ

システムのセットアップが終了した後、オフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。システム情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧(リストア)できなくなります。次の手順に従ってバックアップをしてください。

EXPRESSBUILDER(SE)CD-ROMからシステムを起動して操作します。EXPRESSBUILDER(SE)CD-ROMから起動させるためには、事前にセットアップが必要です。5章を参照して準備してください。

1. 3.5インチフロッピーディスクを用意する。
2. EXPRESSBUILDER(SE) CD-ROMを本体装置のCD-ROMドライブにセットして、再起動する。

   EXPRESSBUILDER(SE)から起動して「EXPRESSBUILDER(SE)トップメニュー」が表示されます。
3. 「ツール」—「オフライン保守ユーティリティ」を選ぶ。
4. [システム情報の管理]から[退避]を選択する。

   以降は画面に表示されるメッセージに従って処理を進めてください。

続いて管理PCに本装置を監視・管理するアプリケーションをインストールします。次ページを参照してください。

二重化構成について

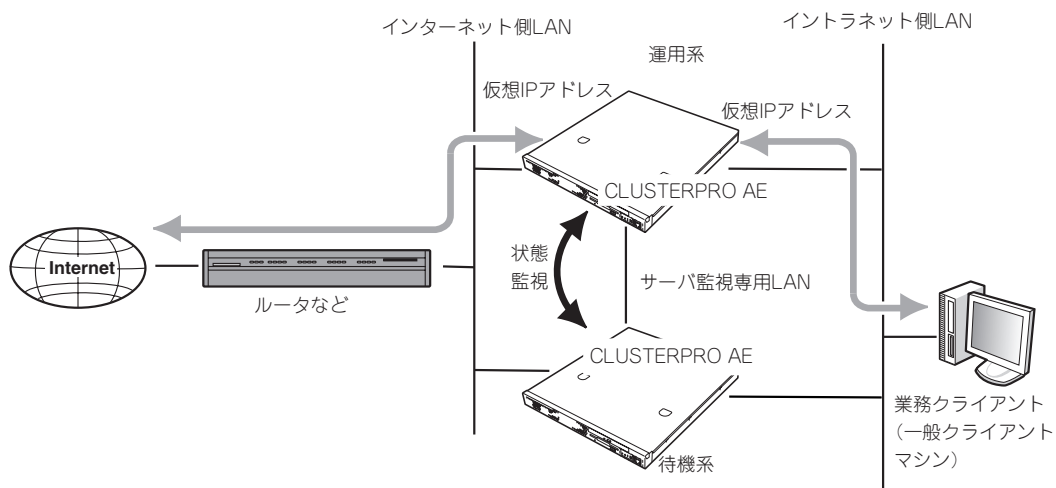
ここではExpress5800/SG300を2台使用して、二重化構成を構築するための手順について説明します。

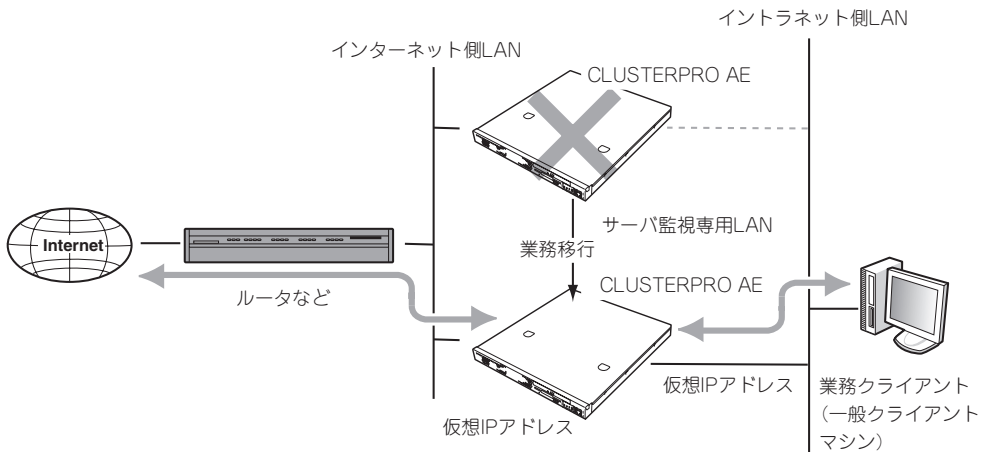
動作概要

Express5800/SG300を二重化することで1台が障害などにより停止しても、もう1台のExpress5800/SG300へ自動的に引き継ぐことにより、障害時の業務停止時間を最小限に抑えることができます。
また、運用系のプロセスの異常を検出した場合や設定されたIPアドレスとの通信が途絶した場合にも、待機系に業務を引き継ぐことが可能です。

以下の仕組みで二重化を実現しています。

● **通常運用時**

- 運用系側で有効にした仮想IPアドレスを使用してインターネット側とイントラネット側の双方からアクセスします。
- 運用系と待機系は互いに状態を監視をします。

- **運用系サーバ障害時**
  - 待機系のFirewallが運用系のダウンを検出します。
  - 運用系のFirewallが仮想IPアドレスを無効にします。
  - 待機系のFirewallが仮想IPアドレスを有効にします。
  - インターネット側とイントラネット側の双方からのアクセスは仮想IPアドレスを使用しているため、切り替わり*に伴う設定の変更をする操作を必要としません。

    * 切り替わる前の通信は途絶えます。

DMZを使用する場合もイントラネット、インターネット同様に仮想IPアドレスが引き継がれます。

初期セットアップ

はじめに2台のExpress5800/SG300を二重化構成で動作させるための設定をします。
購入後、初めてのセットアップで二重化構成を使用する場合は、初期導入設定用ディスクを使った初期セットアップの中で、以下に示す項目について設定します。

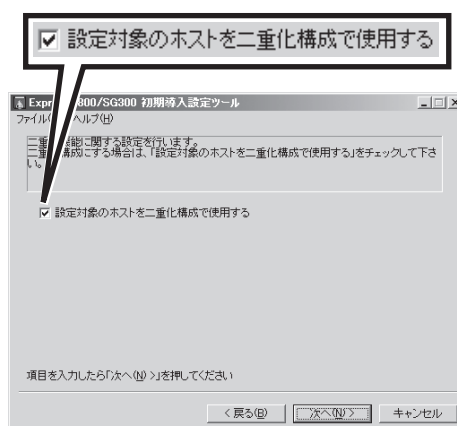
すでに運用しているExpress5800/SG300を二重化構成にする場合や再度構成し直す場合は、Management Consoleを使用します。詳しい手順については、以下のインターネットホームページで記載しています。参照してください。

http://www.express.nec.co.jp/care/user/InterSec_guide.html

(上記URLが変更された場合には、http://nec8.com/からユーザーズガイド配布ページを参照してください。)

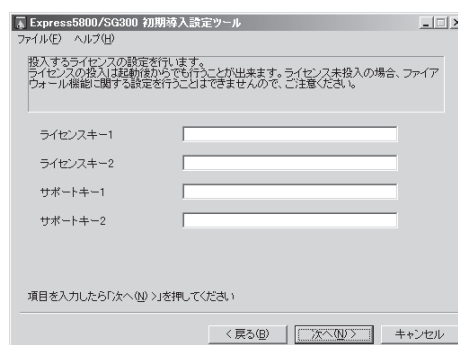
● **設定対象のホストを二重化構成で使用する**

この設定は運用系、待機系の両方で必要な手順です。

二重化構成でExpress5800/SG300を使用するかどうかを設定する項目があります。[設定対象ホストを二重化構成で使用する]にチェックをして、初期導入設定用ディスクを作成してください。

● **ライセンスキーとサポートキーの入力**

運用系と待機系用のライセンスキーとサポートキーを入力します。

運用系と待機系の2つのライセンスキーとサポートキーの入力が必要です。どちらか一方のみを入力すると正しく二重化を構成することはできません。

システムのセットアップ

二重化のための詳細セットアップ

2台のExpress5800/SG300を二重化するためには最低限、次の条件を満たしていないと正しく動作しません。

- 運用系と待機系の二重化基本設定とセキュリティポリシーの設定内容が完全に一致していること（Express5800/SG300本体に割り当てるIPアドレスなどのシステム基本設定は除く）
- 運用系と待機系のライセンスキーとサポートキーがそれぞれのExpress5800/SG300に投入されていること
- 運用系と待機系とも二重化機能サービスが起動していること

運用系と待機系の二重化基本設定とセキュリティポリシーの設定を完全に一致させるために、はじめに一方（運用系）のExpress5800/SG300の基本設定とセキュリティポリシーの設定を完了させ、バックアップ機能を使用して、その内容を任意の場所に保存し、もう一方（待機系）のExpress5800/SG300にリストアします。
次に簡単なセットアップの流れを示します。詳しくは、以下のインターネットホームページで記載しています。参照してください。

http://www.express.nec.co.jp/care/user/InterSec_guide.html

（上記URLが変更された場合には、http://nec8.com/からユーザーズガイド配布ページを参照してください。）

二重化構成をセットアップする場合、および二重化構成を解除する場合（単体サーバとして使用する場合）は、必ず「かんたん設定」をやり直してください。設定の中で仮想IPアドレスなどが正しく設定されていることを確認してください。

スタート

初期導入設定用ディスクによる設定

☞48・75ページ

▽

システムの基本設定

☞60ページ

▽

二重化の詳細設定

☞79ページ

▽

二重化サービスの起動

☞78ページ

▽

状態の確認

[ONLINE]になっていること

☞81ページ

▽

かんたん設定によるセットアップ

[ファイアウォール]→[かんたん設定]

☞4章

▽

ファイアウォールの詳細設定

[ファイアウォール]→[詳細設定]

☞4章

▽

システム情報のバックアップ

[システム]→[バックアップ/リストア]→
任意のバックアップ先
※　基本設定画面での設定内容は含めない

☞69ページ

▽

ファイアウォール設定のバックアップ

[ファイアウォール]→[バックアップ/リストア]→データと設定を選択→任意のバックアップ先

☞71ページ

▽

二重化サービスの停止

☞78ページ

右上に続く

続き ▽

システム情報のリストア

[システム]→[バックアップ/リストア]→
[ファイルを指定してリストア]

☞88ページ

▽

システムの基本設定

☞60ページ

▽

ファイアウォール設定のリストア

[ファイアウォール]→[バックアップ/リストア]→ファイルを選択

☞90ページ

▽

二重化の詳細設定

☞79ページ

▽

二重化サービスの起動

☞78ページ

▽

状態の確認

[ONLINE]になっていること

☞81ページ

▽

二重化サービスの起動

☞78ページ

- [サービス]→[二重化機能]→[詳細設定]→[自動フェイルバック]が[オート]の場合
  <自動フェイルバックが発生>
- [サービス]→[二重化機能]→[詳細設定]→[自動フェイルバック]が[マニュアル]の場合
  <手動で切り替える>

☞84ページ

▽

状態の確認

運用系: [ONLINE]になっていること
待機系: [OFFLINE]になっていること

☞81ページ

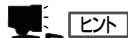
■：運用系　■：待機系　□：両系

二重化サービスの(再)起動と停止

二重化サービスの起動、または再起動、停止の方法について説明します。操作画面は、Management Consoleの[サービス]アイコンをクリックすると表示されます。

1. Express5800/SG300のManagement Consoleに接続し、左側のメニューから[サービス]アイコンをクリックする。

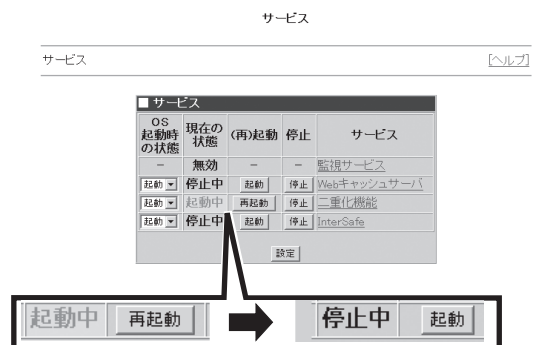
2. [二重化機能]の行の[(再)起動]の項目にある[起動]をクリックする。

   [現在の状態]が[停止中]から[起動中]に、[(再)起動]のボタンが[起動]から[再起動]に切り替わります。

   ヒント

   [OS起動時の状態]でシステムの起動時にサービスの起動を連動させるかどうかを選択することができます。運用する環境に合わせて設定してください。設定を変更した場合は、その設定を有効にするために、[設定]を必ずクリックしてください。

以上でサービスは起動しました。

二重化のサービスをいったん停止する場合は、[停止]をクリックします。
再起動したい場合は、[再起動]をクリックしてください。

[停止]をクリックした場合の例

二重化機能の詳細設定

二重化機能を使用する際に必要なさまざまな設定を変更することができます。設定画面は、Management Consoleの[サービス]アイコンをクリックすると表示されます。

1. Express5800/SG300のManagement Consoleに接続し、左側のメニューから［サービス］アイコンをクリックする。

2. ［サービス］の項目から［二重化機能］をクリックする。

3. ［詳細設定］をクリックする。

   詳細設定画面が表示されます。項目と意味については次ページの表を参照してください。

   重要

   二重化設定で割り当てる仮想IPアドレスが、初期導入設定で割り当てたIPアドレスと重複しないよう注意してください。

項　目	説　明
ハートビート送信間隔	ハートビートの送信間隔（秒）を指定します。
ハートビートタイムアウト時間	ハートビートが途絶えて相手側がダウンしたと認識するまでの時間(秒)を指定します。ハートビート送信間隔より大きい値を指定してください。
相手サーバ起動待ち時間	起動時に相手側の起動時間を待ち合わせる時間（秒）を指定します。ハートビートタイムアウト時間より大きい値を指定してください。
内部通信用TCPポート番号	お互いが通信しあうためのTCPのポート番号を指定します。
内部通信用UDPポート番号	お互いが通信しあうためのUDPのポート番号を指定します。
サーバ1ホスト名	ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。
サーバ2ホスト名	
サーバ1のインタコネクトアドレス	相手側を監視するためのアドレスとネットマスクを入力します。
サーバ2のインタコネクトアドレス	
仮想IPアドレス	二重化機能を使用する場合、Express5800/SG300へのアクセスは原則仮想IPアドレスを使用する必要があります。 サーバ間監視専用インタフェースを除く全インタフェースに仮想IPアドレスを設定してください。
監視対象アドレス	監視対象として設定されたIPアドレスとの通信が途絶した場合、待機系にフェイルオーバが行われます。本項目の設定は省略することができます。
運用系サーバ	2台のうちから運用系を指定します。指定しなかった方が、待機系となります。
自動フェイルバック	自動フェイルバックを行うかどうか設定します。自動フェイルバックを「オート」にした場合、運用系ダウン後、待機系に業務が引き継がれ、運用系が復帰（起動）すると、自動的に運用系に業務を戻します。 「マニュアル」にした場合は、Management Consoleから切り替えます。この後の「手動による切り替えとサービスの停止」を参照してください。

4. ［設定］をクリックする。

   操作結果通知で成功の通知があった場合は、［戻る］をクリックして、次の手順に進んでください。何らかのエラーがあるとその内容が表示されます。［戻る］をクリックした後、メッセージに従って設定し直してください。

■ 操作結果通知

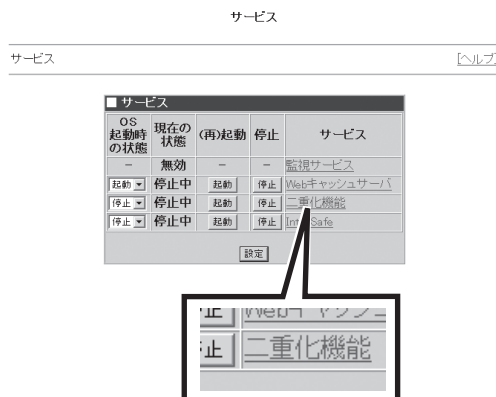
二重化設定情報の変更が成功しました。

戻る

状態の確認

二重化を構成しているExpress5800/SG300が互いに正しく通信できているかどうかや、自分自身の二重化に関する状態を確認します。

1. Express5800/SG300のManagement Consoleに接続し、左側のメニューから[サービス]アイコンをクリックする。

2. [サービス]の項目から[二重化機能]をクリックする。

3. [ステータス確認および二重化切替]をクリックする。

状態表示画面が表示されます。項目と意味については次ページを参照してください。

「ERROR」や「UNKNOWN」の表示がある場合は、前述の「サービスの起動と詳細設定」で詳細設定の内容を確認し直してください。

ただし、二重化の設定中は、片方が「UNKNOWN」と表示される場合がありますが、設定完了後に表示されていなければ問題ありません。

① 運用系と待機系に付けたサーバ名。先頭にアスタリスク（✱）がついている方が現在状態確認画面を表示中のExpress5800/SG300。

② サーバの状態を示す。
  ONLINE:　ハートビートを受信している。
  OFFLINE:　ハートビートを受信していない。

③ 二重化を構成するグループとしての状態を表示します(Express5800/SG300で使用するグループはgroup0の1つのみです)。
  ONLINE:　正常
  OFFLINE:　停止
  ERROR:　異常
  UNKNOWN:　不明

④ フェイルオーバポリシを示す。
  1st:　運用系。
  2nd:　待機系。

⑤ グループの起動が許可されているかどうかを示す。
  ALLOW:　許可
  DENY:　禁止
  UNKNOWN:　不明

⑥ IPWリソースの起動種別と状態、リソース監視アドレスを示す。
  <A>:　全サーバ起動
  <U>:　単サーバ起動
  ONLINE:　正常
  OFFLINE:　停止
  ERROR:　異常
  UNKNOWN:　不明

⑦ FIPリソースの起動種別と状態、リソース設定アドレスとネットマスクを示す（その他は⑥と同じ）。

⑧ EXECリソースの起動種別と状態、リソース起動/停止時実行パスを示す（以降の表示以外は⑥と同じ）。
  S: 起動時実行パス（監視なし）
  W: 起動時実行パス（監視あり）
  E: 停止時実行パス

フェイルオーバとフェイルバック

二重化構成で運用中、待機側は、運用側のハートビートが詳細設定で決めた時間を超えて途絶えると、運用側が故障したか、または運用側のネットワークに何らかの障害が発生したと認識し、自動的に業務を待機側へと切り替えます(フェイルオーバ)。

元の運用側の障害が取り除かれ、現在の運用側(元の待機側)にハートビートの受信が確立したときは、詳細設定での設定内容に従って運用の切り替え(フェイルバック: 元の運用側への切り戻し)をします。

- **オートの場合**

  自動的に元の運用側に切り替わり、現在の運用側は待機側へと切り替わります。

- **マニュアルの場合**

  Management Consoleを使用して切り替え操作をしない限り切り替わりません。詳しくは、この後の「手動による切り替えとサービスの停止」を参照してください。

運用系サーバにおいて障害を検出した場合には、フェイルオーバが発生し、待機系サーバへ業務が切り替わります。その際に基本設定画面で指定した管理者のE-mailアドレス宛にメールが送信されます。以下に通知されるメッセージの例を示します。

- **ダウンしたときのメッセージ**

```
Subject: WARNING: [group0] is downed
!!WARNING!!
[group0] is not active on Firewall(firewall.nec.co.jp[192.168.1.126]).
Urgently check it.
If you recieved a previous message "NOTICE: [group0] changes
to the active firewall" from firewall.nec.co.jp[192.168.1.126],
both groups are downed.
Urgently check both groups!!
```

- **フェイルオーバしたときのメッセージ**

```
Subject: NOTICE: [group0] chnges to the active firewall
!!NOTICE!!
[group0] chnges to the active
firewall(firewall.nec.co.jp[192.168.1.126]).
Urgently check another failed firewall.
```

重要

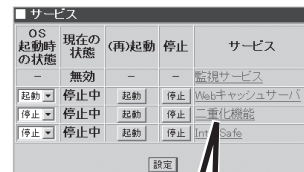
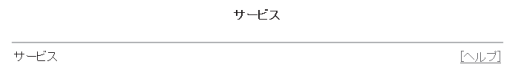
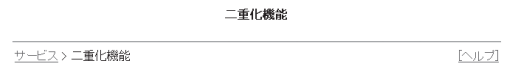
- **ダウンした要因がネットワークの通信障害などの場合、ダウンしたときのメッセージがサーバ内に滞留し、障害復旧後に送信されることがあります。メッセージを受信したら必ずその発信時刻を確認するようにしてください。**
- **メールを受信したらExpress5800/SG300の状態を確認し、システムログ(syslog)などからフェイルオーバが発生した要因を確認し、必要な対処を行ってください。メッセージ内容、対処方法等は付録B「二重化機能のログメッセージ」を参照してください。**

監視対象IPアドレスとの通信途絶、またはFirewallモジュールが異常停止し、待機系に業務を引き継いだ場合、以後、そのサーバ上での業務の起動が拒否されるようになります。業務の起動拒否状態は、[サービス]→[二重化機能]→[状態表示] 画面のグループ起動の許可/禁止を示す[STARTING]行で確認することができます。

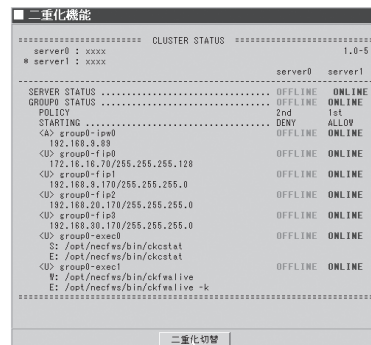
手動による切り替え

待機側に切り替わった元の運用側をもう一度運用側に手動で切り替えるには、Management Consoleを使用します(詳細設定で自動的に切り替えることもできます)。

1. Express5800/SG300のManagement Consoleに接続し、左側のメニューから[サービス]アイコンをクリックする。

2. [サービス]の項目から[二重化機能]をクリックする。

3. [ステータス確認および二重化切り替え]をクリックする。

4. 状態表示に「ERROR」や「UNKNOWN」という表示がないことを確認する。

5. [二重化切替]をクリックする。

6. 約10秒後、[最新情報に更新]をクリックして、切り替えが正しく完了していることを確認する。

単体構成への切り替え

二重化構成をやめる場合は、次の手順に従ってください。

1. 待機側のExpress5800/SG300のネットワークケーブルを取り外し、ネットワークから切り離す。

2. 運用側のExpress5800/SG300のManagement Consoleに接続し、左側のメニューから[ファイアウォール]アイコンをクリックする。

3. [ルール設定]の[詳細設定]をクリックし、ファイアウォールメニュー画面し、VPNで二重化の仮想IPを利用しているものを削除する。

4. 運用側のExpress5800/SG300の二重化サービスを停止する。

   78ページを参照してください。

5. 運用側で[ファイアウォール]アイコンをクリックし、[状態表示]をクリックする。

6. [再起動する](または[起動する])をクリックする。

7. 運用側で[基本設定]アイコンをクリックし、[基本設定]画面を表示する。

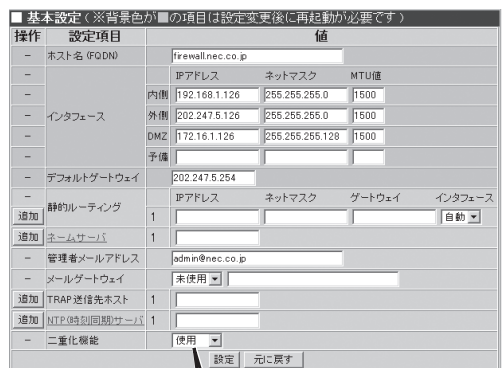
8. [二重化機能]のプルダウンメニューを[使用]から[未使用]に切り替え、[設定]をクリックする。

9. 運用側で「かんたん設定」を実行する。

   詳しくは4章を参照してください。

10. 必要に応じて運用側で「詳細設定」を実行する。

    詳しくは4章を参照してください。

11. 必要に応じて待機側も手順2～10と同様のセットアップをする。

注意・制限事項

- Express5800/SG300 本体が2台必要です。また、ライセンスはそれぞれの実IPアドレスで申請する必要があります。
- 二重化構成でフェイルオーバが発生した場合、接続されていたセッションは切断されます。
- 自動フェイルバックが設定されている場合、運用系サーバの再起動後、自動的に運用系サーバで業務が開始されます。自動フェイルバックが設定されていない場合は、待機系サーバで業務が起動されたままになり、運用系サーバの方が待機状態になります（運用系、待機系の逆転）。運用系サーバに業務を切り替える場合は「手動による切り替え」を参照して切り替えを実行する必要があります。
- 待機系で監視対象IPアドレスとの通信途絶が発生している場合、運用系でリソース異常が発生しても待機系サーバに業務は引き継がれません。ただし、この場合でも「手動による切り替えとサービスの停止」を参照して切り替えることはできます。
- ソフトウェアのアップデートやデータのリストアは待機系、運用系の順番で実行してください。
- 二重化を構成した後、および解除した後は必ず「かんたん設定」を実行してください。また、かんたん設定の中でインタフェースに関する設定が正しいことを確認してください。
- ネットワークを円滑に運用するために、フェイルオーバ後は速やかに障害の原因を取り除き二重化構成に戻してください。

再セットアップ

再セットアップとは、システムの破損などが原因でシステムが起動できなくなった場合などに、添付の「バックアップCD-ROM」を使ってハードディスクを出荷時の状態に戻してシステムを起動できるようにするものです。以下の手順で再セットアップをしてください。

システムの再インストール

ここでは、システムの再インストールの手順について説明します。

再インストールを行うと、装置内の全データが消去され、出荷時の状態に戻ります。必要なデータが装置内に残っている場合、データをバックアップしてから再インストールを実行してください。

再インストールの準備

Express5800/SG300の電源がOFFの状態で、管理クライアントをExpress5800/SG300背面のLANポートインタフェース(内部ネットワーク用)にクロスケーブルで接続してください。また、内部ネットワークに接続する場合は、ハブなどにLANケーブルで接続してください。

Express5800/SG300との接続に必要なもの

- 管理クライアント
- LANケーブル

再インストールに必要なディスク

- バックアップCD-ROM
- 再インストール用ディスク
- 初期導入設定用ディスク

その他、バックアップしたデータがある場合は、あらかじめ管理クライアント上に準備してください。

再インストール手順

再インストールではExpress5800/SG300本体を再インストールした後、システムの基本情報とポリシールールの再設定を行う必要があります。

システムを新たにセットアップする場合は、システムの再インストールを行った後、前述の「セットアップ」ならびに4章の「かんたん設定ウィザード」を参照して、再度システムの基本設定とセキュリティポリシーのセットアップをしてください。

既存の環境でシステムの基本情報とセキュリティポリシーのバックアップを作成している場合、以下の手順でシステムを既存の環境へ再設定することができます。

システムの再インストール

1. Express5800/SG300の電源をONにし、前面にあるフロッピーディスクドライブに再インストール用ディスクを、CD-ROMドライブにバックアップCD-ROMをセットする。

   自動的にバックアップCD-ROMからのインストールが始まります。
   インストールは約10分で完了します。
   インストールを完了すると、CD-ROMドライブからバックアップCD-ROMが排出されます。
   Express5800/SG300は、電源が入った状態で、システムが停止している状態になります。

2. バックアップCD-ROMおよび再インストール用フロッピーディスクを取り出した後、POWERスイッチを押して電源をOFFにする。

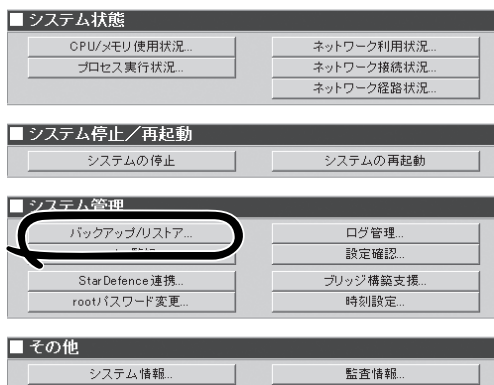
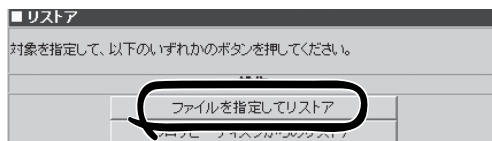
システム基本情報の再設定

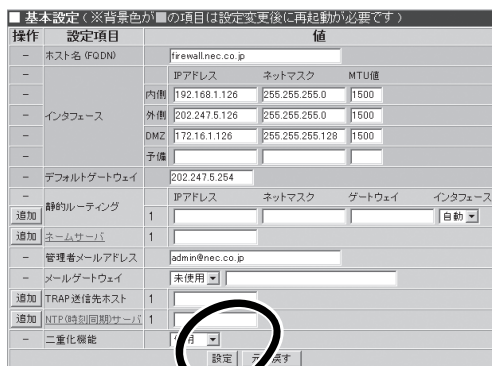
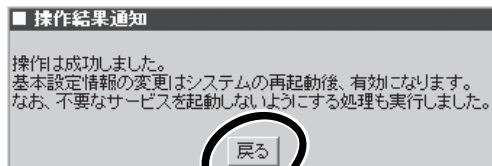
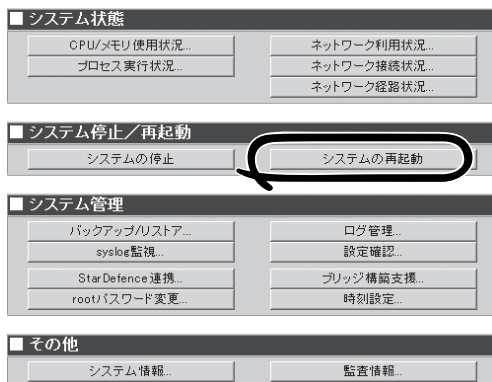
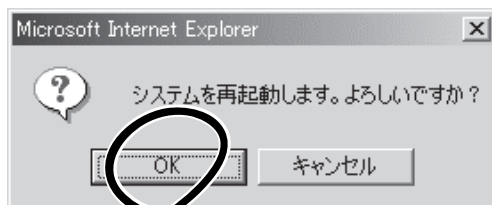
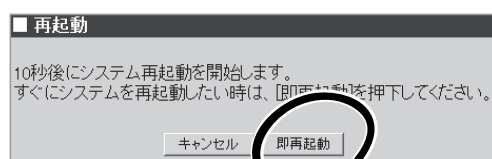
1. 初期導入設定用ディスクをセットした後、POWERスイッチを押して電源をONにする。

   初期導入設定用ディスクは、初期導入設定用ツールで作成済みのものを使用してください。

2. しばらく(3分程度)してから、管理クライアントのウェブブラウザを立ち上げ、Management Consoleへ接続し、左側のメニューから[システム]アイコンをクリックする。

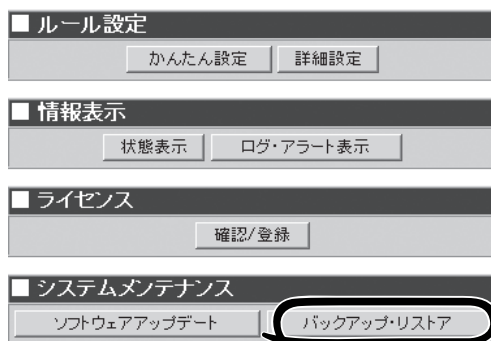
   接続については、4章を参照してください。

3. [バックアップ/リストア]をクリックする。

4. ［ファイルを指定してリストア］を選択し、バックアップファイルを指定してリストアする。

5. 左側のメニューの［基本設定］アイコンをクリックし、［設定］をクリックする。

   バックアップファイルが反映されます。

   バックアップファイルが正常に反映されると、右の画面が表示されます。

6. 左側のメニューの［システム］アイコンを選択し、［システムの再起動］をクリックする。

7. 「システムを再起動します。よろしいですか？」というメッセージが表示されたら、［OK］をクリックする。

8. 再起動画面が表示されたら、［即再起動］をクリックし、再起動する。

セキュリティポリシーのリストア

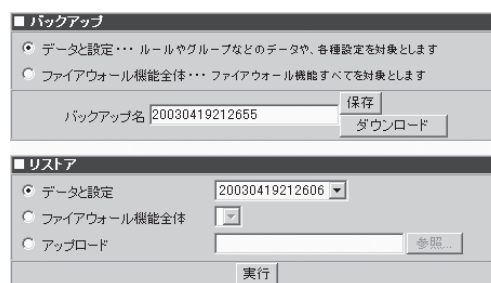
1. 管理クライアントでブラウザを立ち上げ、Management Consoleへ接続し、左側のメニューから[ファイアウォール]アイコンをクリックする。

2. 画面右側に表示される[バックアップ・リストア]をクリックする。

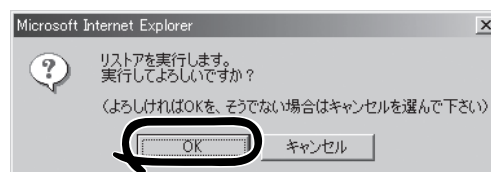
   バックアップリストア画面が表示されます。

3. リストアするバックアップファイルを選択する。

   Express5800/SG300本体にあるバックアップファイルをリストアする場合は、リストアメニューの「データと設定」のラジオボタンを選択します。右のプルダウンメニューより、バックアップファイルを選択し、[実行]をクリックします。

   管理クライアントにあるバックアップファイルをリストアする場合は、リストアメニューの「アップロード」のラジオボタンを選択します。[参照]をクリックし、バックアップファイルを選択してから[実行]をクリックします。

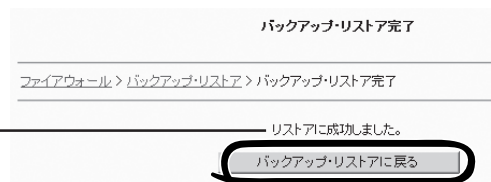
   [実行]をクリックすると確認メッセージウィンドウが表示されます。

4. [OK]をクリックする。

   しばらくすると、バックアップ・リストア完了画面が表示されます。

5. 実行結果を確認後、[バックアップ・リストアに戻る]をクリックする。

バックアップ・リストア完了

ファイアウォール > バックアップ・リストア > バックアップ・リストア完了

実行結果が表示される ― リストアに成功しました。

バックアップ・リストアに戻る

残りのタスク

72ページを参照して、ESMPRO/ServerAgnetのセットアップとマザーボード情報のバックアップを必要に応じて行ってください。

4 ファイアウォール機能の設定方法

本章では、ファイアウォール機能の設定方法について説明します。

Management Consoleについて

ここでは、設定管理ツールManagement Consoleへの接続方法とその画面構成について説明します。

Management Consoleの接続

管理クライアントのウェブブラウザを使用して、Express5800/SG300のManagement Consoleへ接続します。なお、ウェブブラウザは、Microsoft Internet Explorer 6.0 SP1(日本語版・Windows版)以上を使用することを推奨します。

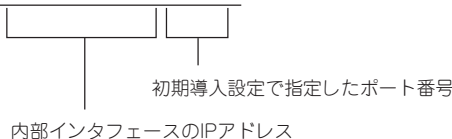
Management Consoleには必ず内部ネットワークの管理クライアントから接続するようにしてください。

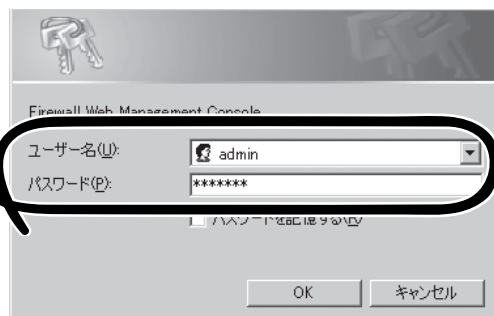
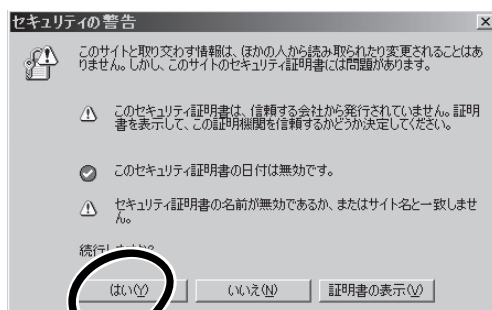
ブラウザが以下のように設定されていることを確認してください。

- JavaScriptを有効にすること
- Cookieを受け入れること

上記のように設定されていないとManagement Consoleが正常に動作しません。

1. Webブラウザを起動し、URLにExpress5800/SG300の内側(管理クライアントが設置されているネットワーク側)のインタフェースのIPアドレスと、初期導入設定ツールで設定したポート番号を指定する。

例） https://192.168.1.126:18000/

接続すると、セキュリティの警告が表示されます。

2. [はい]をクリックする。

ネットワークパスワードの入力画面が表示されます。

セキュリティの警告画面

3. 初期導入設定ツールで設定した管理者アカウント名(ユーザ名)とパスワードを入力する。

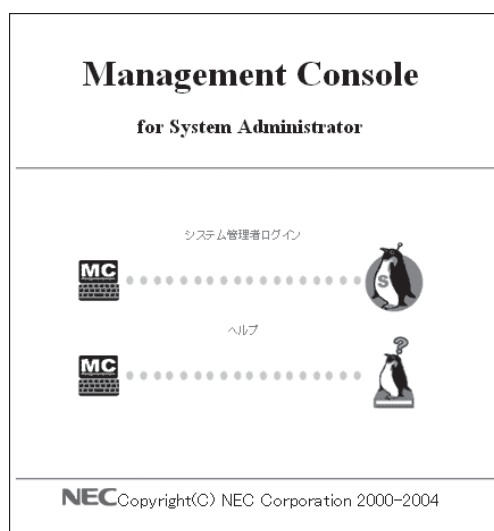
   接続に成功すると、Management Consoleのログイン画面が表示されます。

パスワードの入力画面

4. [システム管理者ログイン]をクリックする。

   Management Consoleのトップ画面が表示されます。

Management Consoleのログイン画面

ファイアウォール機能の設定方法

Management Consoleのトップ画面

管理者はManagement Consoleのトップ画面から各メニューを選択して、Express5800/SG300の設定と管理を行います。各メニューを以下に示します。

Management Consoleのトップ画面

- **基本設定** .... ネットワークインタフェースのアドレスなど、システムの基本的な設定を行います。
- **ファイアウォール** .... アクセス制御のルール定義など、ファイアウォール機能に関する設定と管理を行います。
- **ディスク** .... ディスクの一覧表示や使用量などの確認を行います。
- **サービス** .... オプション製品をインストールしている場合に、そのオプション製品のサービスの起動/停止を行います。
- **パッケージ** .... インストールされているパッケージの情報の確認と、オプション製品のインストールを行います。
- **システムの管理** .... システムの停止/再起動やシステムの状態の確認、およびシステムログの管理などを行います。
- **Management Console** .... Management Consoleのリモートメンテナンス機能に関する設定を行います。

以降、「ファイアウォール」メニューの設定について詳細に説明します。その他のメニューについてはManagement Consoleのヘルプを参照してください。

重要

- **画面上の各ボタンは一度だけクリックしてください。二度以上連続してクリックすると正しく画面が遷移しないことがあります。**
- **ブラウザの戻るボタンやキーボードのショートカットによる戻る機能は使用しないでください。**

かんたん設定ウィザード

Express5800/SG300のファイアウォール機能を利用するには、はじめに「かんたん設定ウィザード」を利用して、ネットワーク構成の選択やフィルタリングの設定などを行う必要があります。
ネットワーク環境が複雑な構成でないときには、このかんたん設定ウィザードに従って設定するだけで、ファイアウォール機能を利用することができます。
かんたん設定ウィザードで設定できる項目を以下に示します。

設定内容の確認 .... すでにかんたん設定ウィザードを使って設定している場合は、設定内容を表示します。

ネットワーク構成の選択 .... Express5800/SG300を導入するネットワークにDMZを構築するかどうか、ブリッジ機能を使うかどうかを選択します。

ネットワークインタフェースの選択 .... Express5800/SG300のインタフェースの設定を行います。

公開サーバの設定 .... 外部ネットワークに公開するサーバ群のIPアドレスやポート番号などの設定を行います。

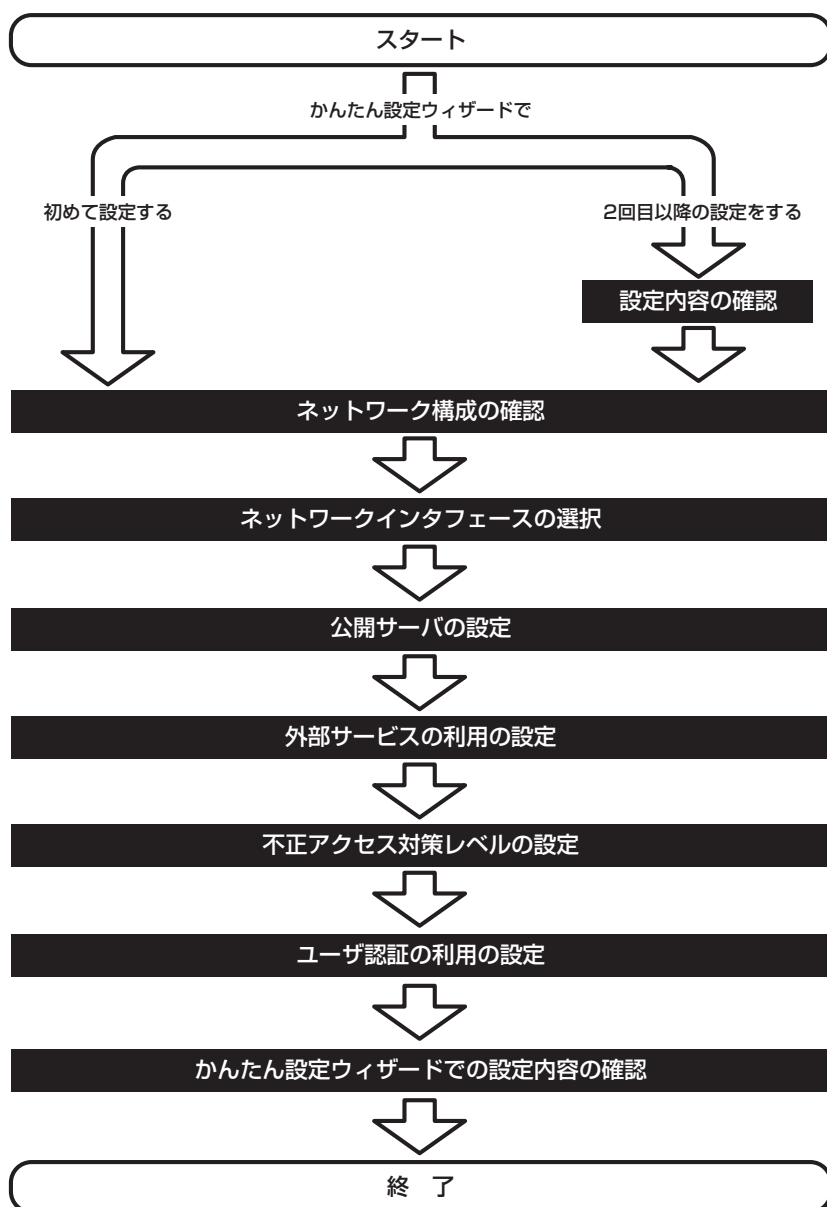
外部サービスの利用の設定 .... 内部ネットワークから外部ネットワークの各種サービスを利用する場合のフィルタリング設定を行います。

不正アクセス対策レベルの設定 .... 外部ネットワークからのアクセス制御のレベルを設定します。

ユーザ認証の利用の設定 .... ユーザ認証機能についての設定を行います。

設定内容の確認 .... かんたん設定ウィザードで設定した内容を確認します。

設定作業の流れ

かんたん設定ウィザードでは、以下のような流れで設定作業を行います。

設定内容の確認

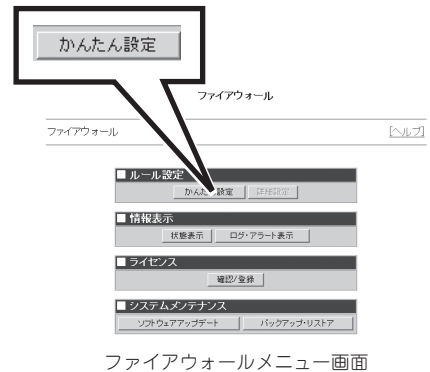
かんたん設定ウィザードですでに設定を行っている場合、現在の設定状況の確認が行えます。ただしセットアップ直後など、一度もかんたん設定ウィザードを利用したことがない場合には、確認画面は表示されずネットワーク構成の選択画面に進みます。

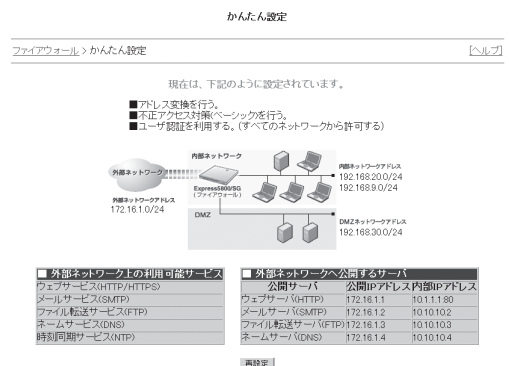
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[かんたん設定]をクリックする。

   設定内容確認画面が表示されます。

ファイアウォールメニュー画面

3. 設定内容確認画面から以下の項目を確認する。

   - NAT/NAPTによるアドレス変換の設定の有無
     Express5800/SG300がアドレス変換を行うかどうか表示します。
     ブリッジ構成の場合は、「ブリッジ機能を利用する」と表示されます。
   - 不正アクセス対策レベル
     不正アクセス対策レベルを表示します。
   - ユーザ認証
     ユーザ認証を利用するかどうかを表示します。
   - ネットワーク構成
     ネットワークの構成、外部ネットワークアドレス、内部ネットワークアドレス、DMZネットワークアドレスを図で表示します。
   - 外部ネットワーク上の利用可能サービス
     内部ネットワークから利用できる外部ネットワーク上のサービスを一覧表示します。
   - 外部ネットワークへ公開するサーバ
     外部ネットワークから利用できる内部ネットワーク上のサーバと、そのサーバの公開IPアドレス、内部IPアドレスを一覧表示します。

設定内容確認画面

4. [再設定]をクリックする。

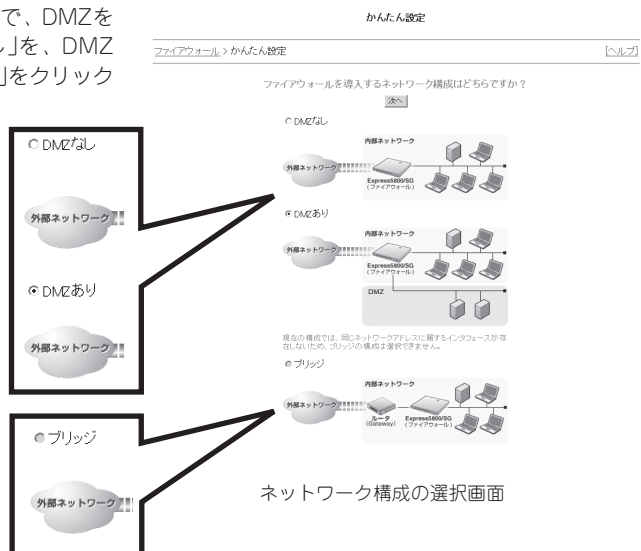
   ネットワーク構成の選択画面が表示され、ネットワーク構成の選択に進みます。

ネットワーク構成の選択

ネットワーク構成の選択では、Express5800/SG300を導入するネットワークの構成として、DMZを利用するかどうかを選択します。
ここで、DMZを利用する構成を選択した場合は、Express5800/SG300に接続されたネットワークは、「外部」、「内部」および「DMZ」に分類されます。DMZを利用しない構成やブリッジ構成を選択した場合は、「外部」と「内部」に分類されます。

- 初めてかんたん設定ウィザードを利用するときは、「ファイアウォール」メニューの「ルール設定」から[かんたん設定]をクリックするとネットワーク構成の選択に進みます。
- 2回目以降の設定の場合は設定内容の確認画面から[再設定]をクリックすると、ネットワーク構成の選択に進みます。

1. ネットワーク構成の選択画面で、DMZを利用しない場合は「DMZなし」を、DMZを利用する場合は「DMZあり」をクリックする。
   Express5800/SGをブリッジとして接続する場合は、[ブリッジ]をクリックする。

ネットワーク構成の選択画面

2. [次へ]をクリックする。

   インタフェース選択画面が表示され、ネットワークインタフェース選択に進みます。

   ヒント

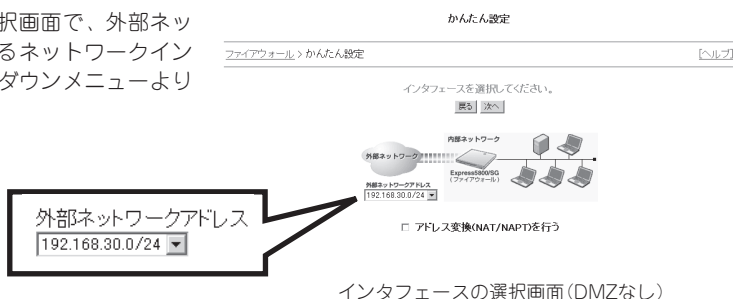
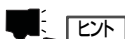
   DMZとは、外部へ公開するサーバを設置するために独立させたセグメントのことで、日本語では「非武装地帯」と訳されます。この部分に外部に公開するサーバを設置し、ファイアウォールでアクセス制御をすることで、安全性を高めることができます。

   たとえば、外部ネットワークからDMZへのアクセスは許可し、DMZから内部ネットワークへのアクセスは許可しない、というように設定すれば、万一、DMZに設置したサーバが第三者に不正侵入されたとしても、内部ネットワークにはアクセスできないため、被害を最小限にとどめることができます。

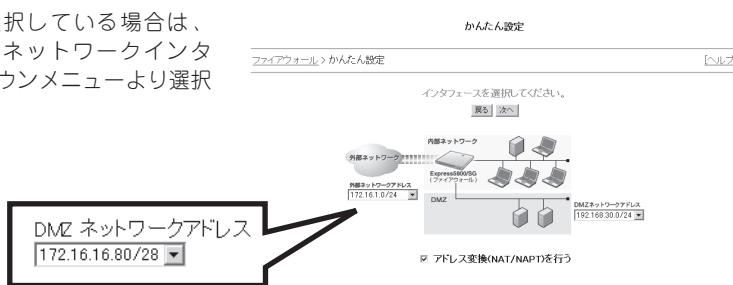
ネットワークインタフェースの選択

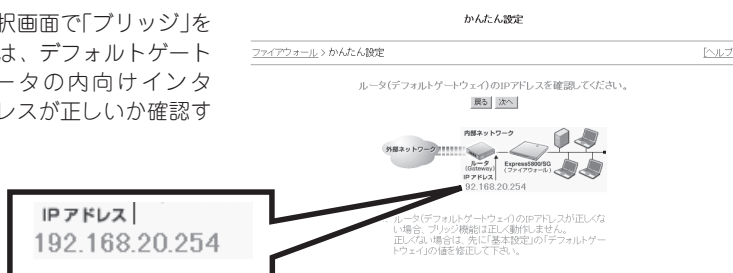
ネットワーク構築の選択で「DMZなし」、「DMZあり」を選択した場合は、外部ネットワークのインタフェースを選択します。通常は変更する必要はありません。「DMZあり」を選択した場合は、DMZのネットワークインタフェースについても選択します。

ネットワーク構築の選択で「ブリッジ」を選択した場合は、デフォルトゲートウェイとなるルータの内向けインタフェースを確認します。

1. インタフェース選択画面で、外部ネットワークにつなげるネットワークインタフェースをプルダウンメニューより選択する。

インタフェースの選択画面(DMZなし)

ヒント

プルダウンメニューに表示されるネットワークインタフェースのIPアドレスは、初期導入設定ツール、またはManagement Consoleの「基本設定」で設定した、ネットワークインタフェースのネットワークアドレスが表示されます。

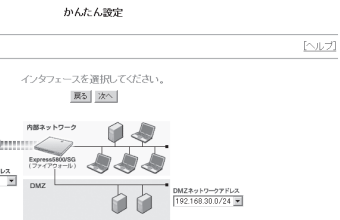
2. 「DMZあり」を選択している場合は、DMZにつなげるネットワークインタフェースをプルダウンメニューより選択する。

インタフェースの選択画面(DMZあり)

3. インタフェース選択画面で「ブリッジ」を選択している場合は、デフォルトゲートウェイとなるルータの内向けインタフェースのIPアドレスが正しいか確認する。

インタフェースの選択画面(ブリッジ)

重要

ルータ(デフォルトゲートウェイ)のIPアドレスが間違っていると、ブリッジ機能は正しく動作しません。IPアドレスが正しくない場合は、「基本設定」でデフォルトゲートウェイのIPアドレスを再設定してから、再度かんたん設定を行ってください。

4. Express5800/SG300上で、外部に公開するサーバ、内部ネットワークの端末のアドレス変換を行う場合には、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックする。

☑ アドレス変換(NAT/NAPT)を行う

インタフェースの選択画面(DMZあり)

ヒント

アドレス変換(NAT/NAPT)とは、内部のネットワークで利用しているIPアドレスが、外部と直接通信できないか、または公開したくないものである場合に、ファイアウォール上でIPアドレスを変換する機能です。たとえば、内部でプライベート(インターネット上のホストとは直接通信できない)IPアドレスを使用している場合に使用します。

ここで、「アドレス変換(NAT/NAPT)を行う」をチェックすると、以降のかんたん設定で公開するサーバを設定する際に、サーバの持つ内部ネットワーク上のIPアドレスとは別に、外部からアクセスするための公開用のIPアドレスを指定できるようになります。外部からこの公開IPアドレスの公開ポートに対してアクセスが行われた場合、ファイアウォール上で宛先IPアドレスを内部IPアドレスに変換します。この機能を「NAT」と呼びます。

また同時に、内部から外部に対してアクセスが行われた場合、ファイアウォール上で送信元IPアドレスをファイアウォールの外部(ネットワークインタフェースに繋がる)IPアドレスに変換します。この機能を「NAPT(またはIPマスカレード)」と呼びます。

5. [次へ]をクリックする。

ウェブサーバ公開の設定画面が表示され、ウェブサーバの設定に進みます。

ヒント

[戻る]をクリックすると、ネットワーク構成の選択画面に戻ります。

公開サーバの設定

外部ネットワークに公開するサーバの設定を行います。設定するサーバを以下に示します。

- ウェブサーバ
- メールサーバ
- ファイル転送サーバ
- ネームサーバ
- その他のサーバ群

ウェブサーバの設定

ウェブサーバの設定では、外部ネットワークに公開するウェブサーバのIPアドレスやポート番号などを登録します。

重要

設定するウェブサーバを、不正アクセス対策や詳細設定メニュー(サーバ公開ルール)で設定するウェブ専用フィルタ機能(外→内)の対象とする場合、該当のウェブサーバは80番ポートである必要があります。80番ポート以外を使用したウェブサーバはウェブ専用フィルタ(外→内)の対象になりません。

1. 外部ネットワークへ公開するウェブサーバの有無を選択する。
   - 公開するウェブサーバ(HTTP)はない
     公開するウェブサーバがない場合は、このラジオボタンをクリックし、手順5に進みます。
   - 公開するウェブサーバ(HTTP)はある
     公開するウェブサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

ウェブサーバ公開の設定画面

2. 「公開IPアドレス」に公開するウェブサーバのIPアドレスを入力し、右端のテキストボックスにポート番号を入力する。

ウェブサーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力し、右端のテキストボックスにポート番号を入力する。

ウェブサーバ公開の設定画面

ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

重要

Express5800/SG300の外部インタフェースのIPアドレスを公開アドレスとして使用することもできますが、ポート番号がユーザ認証ウェブ(112ページ参照)と重複しないよう注意してください。「セキュリティ保護」をチェックした場合、ユーザ認証ウェブのデフォルトのポート番号と同じ443番になることに注意してください。

4. 暗号化して通信を行うHTTPS通信を利用する場合には、「セキュリティで保護」のチェックボックスにチェックする。

ウェブサーバ公開の設定画面

ヒント

- 複数台のウェブサーバを公開する場合は、同様に設定を行ってください。
- かんたん設定ウィザードからは、外部に公開するウェブサーバとして3台までしか設定することができません。もし、4台以上のウェブサーバを設定するときには、「その他のサーバ」として設定するか、157ページの「サーバ公開ルール」および119ページの「サイト共通ルール」を参照してルールを追加してください。

5. [次へ]をクリックする。

メールサーバ公開の設定画面が表示され、メールサーバの設定に進みます。

ヒント

[戻る]をクリックすると、インタフェース選択画面に戻ります。

メールサーバの設定

メールサーバの設定では、外部ネットワークに公開するメールサーバのIPアドレスを登録します。

1. 外部ネットワークへ公開するメールサーバの有無を選択する。
   - 公開するメールサーバ(SMTP)はない
     公開するメールサーバがない場合は、このラジオボタンをクリックし、手順4に進みます。
   - 公開するメールサーバ(SMTP)はある
     公開するメールサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

メールサーバ公開の設定画面

2. 「公開IPアドレス」に公開するメールサーバのIPアドレスを入力する。

メールサーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。

   チェック

   ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

メールサーバ公開の設定画面

ヒント

かんたん設定ウィザードからは、外部に公開するメールサーバとして1台までしか設定することができません。もし、2台以上のメールサーバを設定するときには、「その他のサーバ」として設定するか、157ページの「サーバ公開ルール」および119ページの「サイト共通ルール」を参照してルールを追加してください。

4. ［次へ］をクリックする。

ファイル転送サーバ公開の設定画面が表示され、ファイル転送サーバの設定に進みます。

ヒント

［戻る］をクリックすると、ウェブサーバの設定画面に戻ります。

ファイル転送サーバの設定

ファイル転送サーバの設定では、外部ネットワークに公開するファイル転送サーバのIPアドレスを登録します。

1. 外部ネットワークへ公開するファイル転送サーバの有無を選択する。

   - 公開するファイル転送サーバ(FTP)はない
     公開するファイル転送サーバがない場合は、このラジオボタンをクリックし、手順4に進みます。
   - 公開するファイル転送サーバ(FTP)はある
     公開するファイル転送サーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

ファイル転送サーバ公開の設定画面

2. 「公開IPアドレス」に公開するファイル転送サーバのIPアドレスを入力する。

ファイル転送サーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。

ファイル転送サーバ公開の設定画面

チェック

ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

ヒント

かんたん設定ウィザードからは、外部に公開するファイル転送サーバとして1台までしか設定することができません。もし、2台以上のファイル転送サーバを設定するときには、「その他のサーバ」として設定するか、157ページの「サーバ公開ルール」および119ページの「サイト共通ルール」を参照してルールを追加してください。

4. [次へ]をクリックする。

ネームサーバ公開の設定画面が表示され、ネームサーバの設定に進みます。

ヒント

[戻る]をクリックすると、メールサーバ公開の設定画面に戻ります。

ネームサーバの設定

ネームサーバの設定では、外部ネットワークに公開するネームサーバのIPアドレスを登録します。

1. 外部ネットワークへ公開するネームサーバの有無を選択する。

   - 公開するネームサーバ(DNS)はない
     公開するネームサーバがない場合は、このラジオボタンをクリックし、手順4に進みます。
   - 公開するネームサーバ(DNS)はある
     公開するネームサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

ネームサーバ公開の設定画面

ファイアウォール機能の設定方法

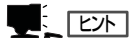
2. 「公開IPアドレス」に公開するネームサーバのIPアドレスを入力する。

ネームサーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。

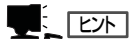
ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

ネームサーバ公開の設定画面

ヒント

かんたん設定ウィザードからは、外部に公開するネームサーバとして1台までしか設定することができません。もし、2台以上のネームサーバを設定するときには、「その他のサーバ」として設定するか、157ページの「サーバ公開ルール」および119ページの「サイト共通ルール」を参照してルールを追加してください。

4. [次へ]をクリックする。

その他の公開サーバの設定画面が表示され、その他のサーバ群の設定に進みます。

ヒント

[戻る]をクリックすると、ファイル転送サーバ公開の設定画面に戻ります。

外部ネットワークに公開するその他のサーバ群の設定

その他のサーバ群の設定では、外部ネットワークに公開するその他のサーバ群のIPアドレスやポート番号などを登録します。

1. これまで設定してきたウェブサーバ、メールサーバ、ファイル転送サーバ、ネームサーバ以外で外部ネットワークへ公開するサーバの有無を選択する。

   - その他の公開するサーバはない
     その他の公開するサーバがない場合は、このラジオボタンをクリックし、手順4に進みます。
   - その他の公開するサーバはある
     その他の公開するサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

その他の公開サーバの設定画面

2. 「公開IPアドレス」に公開するサーバのIPアドレスを入力し、右端のテキストボックスにポート番号を入力する。

サーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換（NAT/NAPT）を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。

   チェック

   ネットワークインタフェースの選択画面において、「アドレス変換（NAT/NAPT）を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

   重要

   Express5800/SG300の外部インタフェースのIPアドレスを公開アドレスとして使用することもできますが、ポート番号がユーザ認証ウェブ（112ページ参照）と重複しないよう注意してください。

サーバ公開の設定画面

ヒント

かんたん設定ウィザードからは、外部に公開するその他のサーバ群として5台までしか設定することができません。もし、6台以上のサーバを設定するときには、157ページの「サーバ公開ルール」および119ページの「サイト共通ルール」を参照してルールを追加してください。

4. [次へ]をクリックする。

外部ネットワーク利用サービス選択の画面が表示され、外部ネットワークのサービスの利用の選択に進みます。

ヒント

[戻る]をクリックすると、ネームサーバ公開の設定画面に戻ります。

外部サービスの利用の選択

内部ネットワークから利用する外部ネットワークのサービスを選択します。選択するサービスを以下に示します。

- ウェブサービス(HTTP/HTTPS)
- メールサービス(SMTP)
- ファイル転送サービス(FTP)
- ネームサービス(DNS)
- 時刻同期サービス(NTP)

1. サービスの利用の有無を選択する。

   ヒント

   かんたん設定ウィザードからは、外部サービスとして上記に示す5つのサービスまでしか設定することができません。もし、これら以外のサービスを利用するときには、119ページの「サイト共通ルール」を参照してルールを追加してください。

外部ネットワーク利用サービス選択の画面

2. [次へ]をクリックする。

   より強固な不正アクセス対策の設定画面が表示され、不正アクセス対策レベルの設定に進みます。

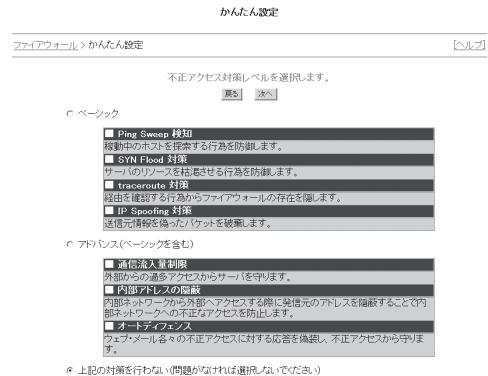
   ヒント

   [戻る]をクリックすると、その他のサーバ群の設定画面に戻ります。

不正アクセス対策レベルの設定

不正アクセス対策のレベルを設定します。対策のレベルには以下の3つがあります。

- ベーシック
- アドバンス
- 上記の対策を行わない

1. 不正アクセス対策レベルを選択する。

より強固な不正アクセス対策の設定画面

それぞれの対策について説明します。

「ベーシック」を選択すると以下の不正アクセス対策を行います。

- Ping Sweep検知
  Ping Sweepとは、Pingを利用してネットワーク上で稼動するホストを調べることで、しばしば攻撃を仕掛ける前の事前調査として行われます。Ping Sweep検知では悪意を持った第三者によるPing Sweepを検知します。
- SYN Flood対策
  SYN Floodとは、攻撃対象のホストに対してSYNパケットを大量に送りつけるDoS攻撃の1つです。SYN Flood対策では悪意を持った第三者からSYN Flood攻撃を受けたとしても、サーバリソースの枯渇を防ぐことが可能です。
- traceroute対策
  ネットワークの経由情報からファイアウォールの所在を隠すことが可能です。
- IP Spoofing対策
  送信元情報を偽ったパケットを破棄することが可能です。

「アドバンス」を選択すると、「ベーシック」レベルの対策に加えて、次の3つの不正アクセス対策を追加します。

- 通信流入量の制限
  Express5800/SG300では外部ネットワークからの過剰なアクセスを制限することが可能です。この機能では、外部ネットワークから受信するパケット量が上限値(70Mbps)を超えたとき、ファイアウォールを越えての新規の接続要求を拒絶します。これにより、DoS攻撃などの悪意を持った過負荷となる通信から内部サーバを保護します。

  パケット量は、宛先や送信元、ポートによらず、受信する全パケットの総量で測ります。パケット流入量の上限値や、制限を掛けるインタフェースの調整は詳細設定の流入量制限ルールから行うことができます。

- 内部アドレスの隠蔽
  SMTP通信について、内部ネットワークから外部ネットワークへアクセスする際に内部ネットワークのアドレスを隠蔽します。これにより、内部ネットワークへの不正アクセスを防ぎます。

  この機能では、IPヘッダのアドレスのほか、HTTPリクエストやSMTPのコマンドとメールヘッダ中に含まれるクライアントのIPアドレスを、Express5800/SG300の外部インタフェースのIPアドレスに書き換えることで、内部ネットワークのアドレスを隠します。また、公開しているメールサーバが外部ネットワークへ送信するIPヘッダやサーバ応答、メールヘッダについても、内部ネットワークのIPアドレスをExpress5800/SG300のIPアドレスに書き換えるなど、適切に処理するので、内部ネットワーク上のメールサーバのアドレス隠蔽も可能です。

- オートディフェンス
  ウェブサービス、メールサービスへの不正アクセスに対して応答を偽装することにより、正規サーバを不正アクセスから守ることが可能です。

  ウェブやメールのポートへ無作為にアクセスして応答するサーバを探し、不正アクセスを試みる不審者に対処する機能です。

  偽装応答に対して続けてアクセスしてきたときや、公開していないサーバのウェブやメールのポートに多数の接続(120秒に1000回以上)を要求してきたときは、不審者とみなして、その送信元からのすべてのアクセスを1時間禁止します。これにより、公開しているサーバへの攻撃を防ぐ可能性を高めます。

「上記の対策を行わない」のラジオボタンを選択すると、Express5800/SG300は上記のいずれの対策も行いません。

重要

- **内部アドレスの隠蔽機能(内部メールサーバのアドレス隠蔽)とオートディフェンス機能の対象ポートは、HTTP(ポート番号80)、SMTP(ポート番号25)です。独自のポート番号やHTTPS(ポート番号443)で公開しているサーバは対象外です。**
- **外部ネットワークから接続されるウェブサーバやメールサーバは、公開サーバとして必ず登録しておいてください。登録していないと、オートディフェンス機能により偽装応答が返ります。**
- **詳細設定のサイト共通ルール設定とサーバ公開ルール設定の各画面にあるウェブ専用フィルタとメール専用フィルタのチェックボックスのチェックを外すとアドバンスレベルの不正アクセス対策の一部の機能が解除されます。逆に、不正アクセスのアドバンスレベルの選択を外すと、詳細設定のウェブ・メール専用フィルタのいくつかのチェックボックスのチェックも外れます。**

ヒント

公開しているウェブサーバやメールサーバへの過剰アクセスを一時遮断する機能は、詳細設定のサーバ公開ルール画面のウェブ専用フィルタとメール専用フィルタの設定から指定できます。

2. [次へ]をクリックする。

ユーザ認証の利用選択画面が表示され、ユーザ認証の利用の有無の設定に進みます。

ヒント

[戻る]をクリックすると、外部ネットワーク利用サービス選択の画面に戻ります。

ユーザ認証の利用の設定

外部ネットワークから内部ネットワークに存在する端末にアクセスするときや、内部ネットワークから外部ネットワークに存在する端末にアクセスするときは、ファイアウォールとなるExpress5800/SG300を介して通信を行います。このとき、ユーザ認証によりユーザごとに使用する通信を許可することができます。ユーザ認証の利用の設定では、ユーザ認証を利用するかどうかを設定します。

リモートアクセスVPNを利用する場合は、「ユーザ認証を利用する」に設定してください。認証の受付は「すべてのネットワークから許可する」に設定してください。

ヒント

ユーザの認証は、「ユーザ設定」で登録するユーザID、パスワードにより認証します。217ページの「ユーザ設定」を参照してください。
また、認証を行ったユーザごとに通信の許可を行う場合は、ユーザをユーザグループに所属させ、該当ユーザグループのグループルールを設定する必要があります。ユーザグループ設定とグループルール設定については、それぞれ235ページと142ページを参照してください。

1. ユーザ認証の利用の有無を選択する。

   - ユーザ認証を利用しない
     ユーザ認証を利用しない場合は、このラジオボタンをクリックし、手順4に進みます。
   - ユーザ認証を利用する
     ユーザ認証を利用する場合は、このラジオボタンをクリックし、手順2に進みます。

ユーザ認証の利用選択画面

2. ユーザ認証ウェブのポート番号を指定する。

   デフォルトでは「443」に設定されています。通常変更する必要はありません。

ユーザ認証の利用選択画面

3. ユーザ認証の受付を設定する。

- 内部ネットワークからのみ許可する
ユーザ認証のためのアクセスを内部ネットワークからのみ受付けます。
- すべてのネットワークから許可する
ユーザ認証のためのアクセスをどこからでも受付けます。

ユーザ認証の利用選択画面

4. [次へ]をクリックする。

設定内容確認画面が表示され、これまでの設定内容の確認に進みます。

ヒント

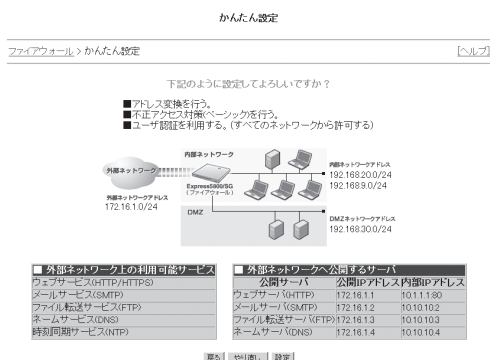
- [戻る]をクリックすると、より強固な不正アクセス対策の設定画面に戻ります。
- ユーザ認証は詳細設定メニューの「認証設定」からも設定することができます。認証設定については、231ページを参照してください。

かんたん設定ウィザードでの設定内容の確認

かんたん設定ウィザードを利用して設定した内容を確認することができます。

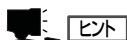
1. 設定内容確認画面から以下の項目を確認する。

設定内容確認画面

- NAT/NAPTによるアドレス変換の設定の有無
  Express5800/SG300がアドレス変換を行うかどうか表示します。
  ブリッジ構成の場合は、「ブリッジ機能を利用する」と表示されます。
- 不正アクセス対策レベル
  不正アクセス対策レベルを表示します。
- ユーザ認証
  ユーザ認証を利用するかどうかを表示します。
- ネットワーク構成
  ネットワークの構成、外部ネットワークアドレス、内部ネットワークアドレス、DMZネットワークアドレスを図で表示します。
- 外部ネットワーク上の利用可能サービス
  内部ネットワークから利用できる外部ネットワーク上のサービスを一覧表示します。
- 外部ネットワークへ公開するサーバ
  外部ネットワークから利用できる内部ネットワーク上のサーバと、そのサーバの公開IPアドレス、内部IPアドレスを一覧表示します。

2. 設定した内容で問題なければ[設定]をクリックする。

   ルール適用画面が表示されます。

設定内容の適用に失敗すると、エラー内容が表示されます。その場合、再度設定をやり直してください。

ヒント

[やり直し]をクリックすると、設定した内容は保持したままかんたん設定ウィザードのネットワーク構成の選択画面に戻り、最初から設定をやり直すことができます。

3. ［戻る］をクリックする。

ファイアウォールメニューに戻ります。

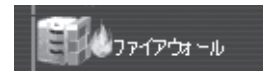
設定内容確認画面

詳細設定メニュー

かんたん設定ウィザードを利用して設定を行った後、細かい設定が必要な場合は、詳細設定メニューを使用します。

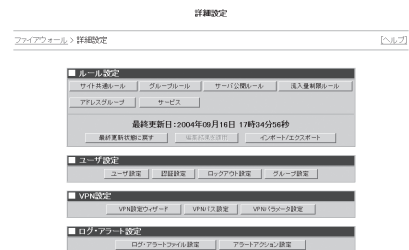
重要 詳細設定を行うには、必ず一度はかんたん設定ウィザードでの設定を行う必要があります。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

   詳細設定メニューからは主に以下の内容を設定することができます。

   - ルール設定
     かんたん設定ウィザードで設定した内容をさらに詳しく設定することができます。
   - ユーザ設定
     ユーザ情報の登録、削除、更新といった管理やユーザ認証の設定を行います。
   - VPN設定
     VPNの詳細設定をすることができます。
   - ログ・アラート設定
     ログファイルやアラートファイルに関連する各種パラメータを設定することができます。

   重要
   「ルール設定」の中で、ボタンの下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。各項目の設定では、設定完了後、[登録]をクリックしますが、この段階では新しい設定内容を作成しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。

ファイアウォールメニュー画面

詳細設定メニュー画面

ルール設定

かんたん設定ウィザードで設定した内容をさらに詳しく設定することができます。
ルール設定では以下の項目を設定します。

サイト共通ルール .... 外部ネットワークと内部ネットワーク、あるいは外部ネットワークとDMZ、さらには内部ネットワークとDMZというように、Express5800/SG300を間に挟んだネットワークをサイトとして管理し、そのサイト内で常時適用されるルールを設定することができます。

グループルール .... サイト共通ルールでの設定に対して、グループ単位で例外的に許可するルールを設定することができます。

サーバ公開ルール .... 外部ネットワークにサーバを公開するための設定やアドレス変換(NAT)などを行うことができます。

流入量制限ルール .... DMZ/内部ネットワークに入ってくるパケット流量を制限することができます。

アドレスグループ .... アドレスごとにグループを作成することができます。サイト共通ルールやグループルールの発信元、宛先に指定することができます。

サービス .... サービスを新たに定義することができます。定義したサービスはサイト共通ルールやグループルールの通信種別に設定することができます。

ルール設定の履歴表示 .... 設定したルールの履歴を表示することができます。

インポート/エクスポート .... 各ルールの設定内容をエクスポートしたり、Express5800/SG300にインポートすることができます。

各ボタンの下に「編集中」と表示されている場合には、各種ルールを編集したままであることを示しています。[編集結果を適用]をクリックすれば、編集内容をExpress5800/SG300に適用することができます。
編集中のルールセットを破棄したい場合には、[最終更新状態に戻す]をクリックすれば、編集中のルールを破棄し、Express5800/SG300に適用した最終のルールセットの状態に戻すことができます。

設定作業の流れ

ここでは、かんたん設定ウィザードで設定をした後、詳細設定メニューを利用してさらに詳細な設定を行う場合の作業の流れを設定事例をもとに説明します。

■ 外部ネットワークから内部ネットワークやDMZ上のサーバへのアクセスを許可するには

1. サーバ公開ルールを設定する。
2. サイト共通ルールを設定する。
   このときNATを利用している場合、宛先は内部IPアドレスを指定します。
3. 詳細設定メニューで、サーバ公開ルールとサイト共通ルールの編集結果を適用する。

■ 内部ネットワークから外部ネットワークへのアクセスを許可するには

1. サイト共通ルールを設定する。
2. 詳細設定メニューで、サイト共通ルールの編集結果を適用する。

■ 認証されたユーザについてのアクセスを許可するには

1. グループ設定で、ユーザのグループを作成する。
2. ユーザ設定で、ユーザを作成してグループに所属させる。
3. グループルールを設定する。
4. 詳細設定メニューで、グループルールの編集結果を適用する。

■ 内部ネットワークユーザが閲覧する外部ネットワークのURLを制限するには

1. サイト共通ルールのウェブ専用フィルタの設定を行う。
2. サイト共通ルールで、「ウェブ専用フィルタを経由して見る」を有効にする。
3. 詳細設定メニューで、サイト共通ルールの編集結果を適用する。

■ 外部ネットワークの特定のメールアドレスからのメールを制限するには

1. サーバ公開ルールのメール専用フィルタの設定を行う。
2. サーバ公開ルールで、「メール専用フィルタを経由して公開する」を有効にする。
3. 詳細設定メニューで、サーバ公開ルールの編集結果を適用する。

サイト共通ルール

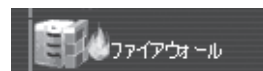
サイト共通ルールとは、Express5800/SG300を導入した環境において、外部ネットワークと内部ネットワーク、あるいは外部ネットワークとDMZ、さらには内部ネットワークとDMZというように、Express5800/SG300を間に挟んだネットワーク内で常時適用されるルールのことです。
サイト共通ルールでは、以下のような設定・管理を行うことができます。

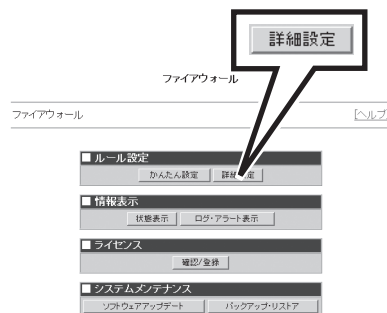
- サイト共通ルールの設定内容の確認
- サイト共通ルールの追加
- サイト共通ルールの削除
- サイト共通ルールの更新
- ルール評価順の入れ替え
- 内部から外部への通信におけるウェブ専用フィルタの設定
- 内部から外部への通信におけるメール専用フィルタの設定

サイト共通ルールの設定内容の確認

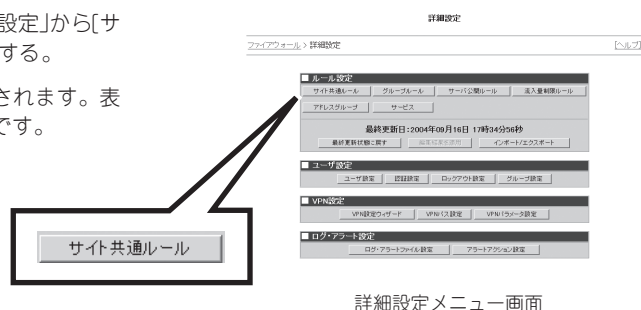
かんたん設定ウィザードから設定したサイト共通ルールや、すでに設定したルールはサイト共通一覧画面から確認することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

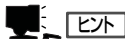
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

ルール設定一覧画面が表示されます。表示される内容は以下の通りです。

詳細設定メニュー画面

項　目	説　明	
No.	ルールの番号です。通信を通すか否かの判定の際は、番号の若いルールから順番に評価した結果、最初にマッチしたルールに基づいて処理されます。	
発信元	パケットの発信元を表すIPアドレス、ネットワークアドレス、あるいは内部、外部、DMZのいずれかです。	
宛先	パケットの宛先を表すIPアドレス、ネットワークアドレス、あるいは内部、外部、DMZのいずれかです。	
通信種別	パケットのプロトコル種別を表します。	
処理		パケットを通します。
		パケットを破棄し、発信元へ応答を返しません。
		パケットを拒否し、発信元へエラーを返します。
記録		通信のログを残します。
		通信のログを残すとともにアラート情報も残します。
	〔空白〕	ログもアラートも残しません。

No.	発信元	宛先	通信種別	処理	記録
1	内部	内部	任意		
2	任意	10.10.10.1	http		
3	任意	10.10.10.2	https		
4	任意	10.10.10.3	smtp		
5	任意	10.10.10.4	ftp		
6	任意	10.10.10.5	dns		
7	内部	外部	http		
8	内部	外部	https		
9	内部	外部	smtp		
10	内部	外部	ftp		
11	内部	外部	dns		
12	内部	外部	ntp		
13	内部	ファイアウォール自身	https		
14	内部	ファイアウォール自身	daytime		

サイト共通ルール設定画面

ヒント

- 画面右上の「設定履歴」をクリックすると、「かんたん設定」と「ルール設定」での設定内容の履歴が表示されます。
- 画面右上の「かんたん設定(ネットワーク構成)の確認」をクリックすると、かんたん設定で設定した内容が別ウィンドウで表示されます。

具体的なサイト共通ルール一覧の事例を示します。

No.	発信元	宛先	通信種別	処理	記録
1	内部	内部	tcpすべて		
2	外部	192.168.30.20	tcpすべて		
3	部門ネット1 部門ネット2	ウェブサーバ	http https		

ルール設定一覧

ルールの1行目:　内部ネットワークにある端末間のすべてのTCP通信を許可することを表します。

ルールの2行目:　外部ネットワークから192.168.30.20のIPアドレスを持つ端末へのTCP通信をすべて拒否し、その通信ログとアラート情報を残すことを表します。

ルールの3行目:　部門ネット1、部門ネット2からウェブサーバへのHTTP通信、HTTPS通信を許可しログを残すことを表します。

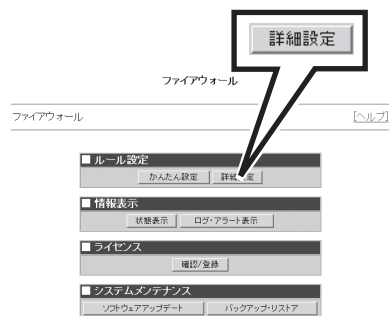
ファイアウォール機能の設定方法

サイト共通ルールの追加

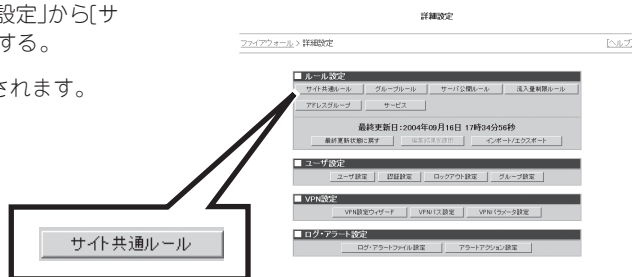
必要に応じてサイト共通ルールを追加することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

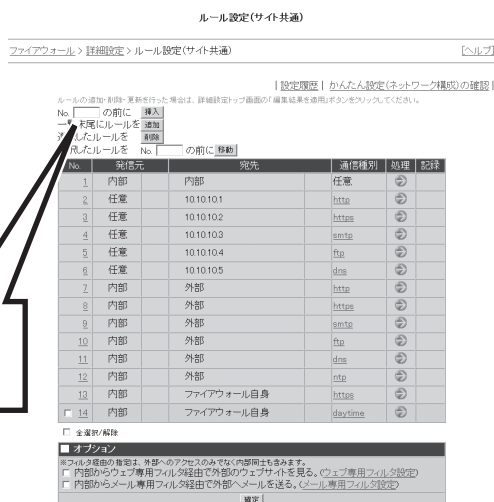
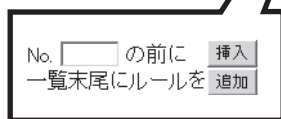
3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   ルール設定一覧画面が表示されます。

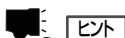
詳細設定メニュー画面

4. 表の途中に挿入する場合は、「No.の前に『挿入』」の「No.」のテキストボックスにルールの番号を入力し、「No.の前に『挿入』」をクリックする。表の末尾に追加する場合は、「一覧末尾にルールを『追加』」をクリックする。

ルール設定追加画面が表示されます。

サイト共通ルール設定画面

チェック

「No.」のテキストボックスに値を入れずに「No.の前に『挿入』」をクリックすると、エラー内容を示す画面を表示します

ヒント

「かんたん設定ウィザード」で設定されたルール(背景ピンク色)の間にも新しくルールを挿入することはできますが、再度「かんたん設定ウィザード」を用いてルールを再生成した場合、追加したルールは一覧の上部に表示され、「かんたん設定ウィザード」で設定したルールよりも評価順が上位になります。

5. ルール設定追加画面に表示される各項目を設定する。

ルール設定追加画面

項　目		説　明
処理	許可	パケットを通します。
	破棄	パケットを破棄し、発信元へ応答を返しません。
	拒否	パケットを拒否し、発信元へエラーを返します。
発信元	ユーザ指定	ユーザの指定した発信元に対し処理を適用します。 テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループは、184ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークからの通信です。
	内部	内部ネットワークからの通信です。
	DMZ	DMZからの通信です。
	任意	発信元に関わらず処理を適用します。
	上記指定以外	チェックボックスをチェックすると、選択した発信元以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を発信元とする通信に対し処理を適用します。
宛先	ユーザ指定	ユーザの指定した宛先に対し処理を適用します。 テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループは、184ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークへの通信です。
	内部	内部ネットワークへの通信です。
	DMZ	DMZへの通信です。
	任意	宛先に関わらず処理を適用します。
	ファイア ウォール自身	ファイアウォール自身への通信です。
	上記指定以外	チェックボックスをチェックすると、選択した宛先以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を宛先とする通信に対し処理を適用します。
通信種別	ユーザ指定	ユーザの指定したプロトコル種別に対して処理を適用します。テキストエリアにプロトコル種別を直接入力するかサービス種別をリストから指定します。サービス種別から指定する場合は、サービスのリストからサービス種別を選択し、[←]をクリックします。クリックするとテキストエリアに選択したサービスが表示されます。サービスのリストには、195ページの「サービス」で登録したものと標準定義サービスが表示されます。
	任意	通信種別に関わらず処理を適用します。
記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート	通信のログを残すとともにアラート情報も残します。

ヒント

- 発信元および宛先が含むアドレスグループのメンバの数の合計は、直接入力したアドレスの数を含めて最大50個までです。
- 通信種別が含むサービスのメンバの数の合計は、直接入力した要素の数を含めて最大50個までです。

6. ［登録］をクリックする。

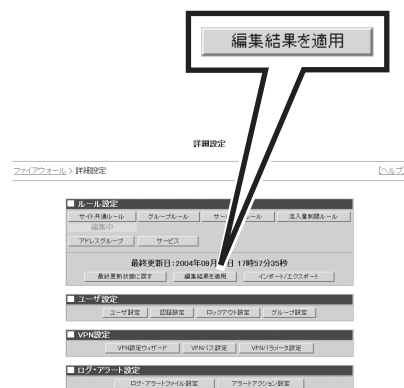
ルール設定追加結果画面が表示されます。

登録に失敗した場合には、エラー内容を示す画面を表示します。

7. ［ルール設定（サイト共通）に戻る］をクリックする。

追加したルールが反映されたルール設定一覧画面が表示されます。

ルール設定追加結果画面

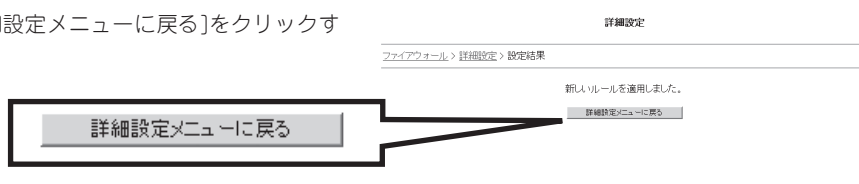
8. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。

詳細設定メニュー

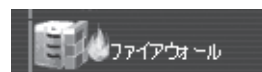
重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの追加前の状態に戻ります。

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

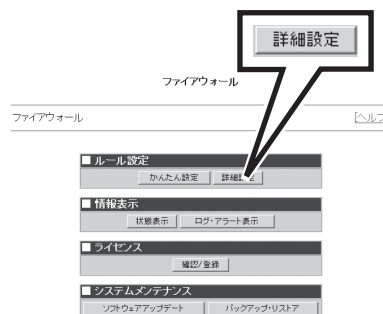
新しく追加したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。

サイト共通ルールの削除

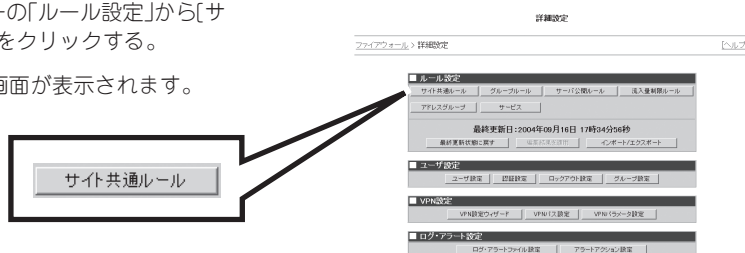
不要になったサイト共通ルールを削除することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

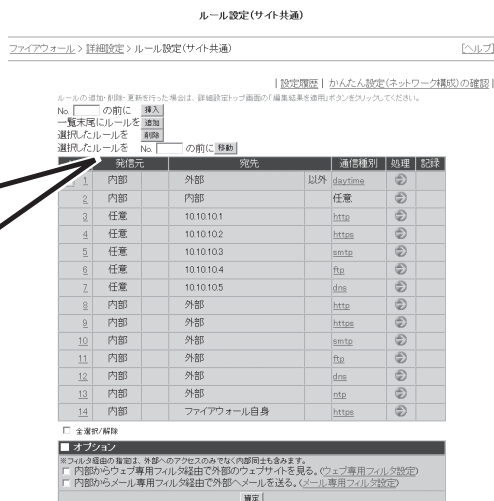
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   ルール設定一覧画面が表示されます。

詳細設定メニュー画面

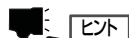
4. 削除したいルールの「No.」の横に表示されるチェックボックスをチェックし、「選択したルールを『削除』」をクリックする。

サイト共通ルール設定一覧画面

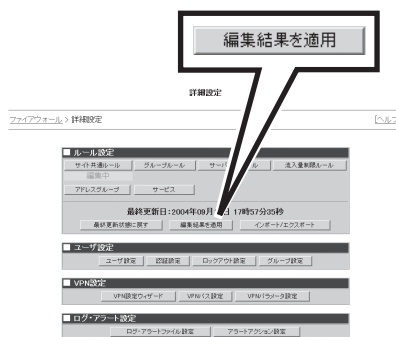
ヒント

- 一覧の背景がピンク色の項目は、「かんたん設定ウィザード」を経由して設定されたルールであることを示しています。このルールについては、サイト共通ルールの設定から削除することはできません。
- 「全選択/解除」のチェックボックスをチェックすると、削除可能なルールのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのルールを削除対象から外すこともできます。

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

   サイト共通ルールが削除され、削除確認の別ウィンドウが閉じます。

   ヒント

   [キャンセル]をクリックすると、削除されずにルール設定一覧画面に戻ります。

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順5で[OK]をクリックしますが、この段階ではルールの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの削除前の状態に戻ります。**

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   ルールの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。

詳細設定

ファイアウォール > 詳細設定 > 設定結果

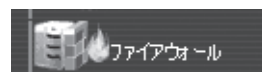
新しいルールを適用しました。

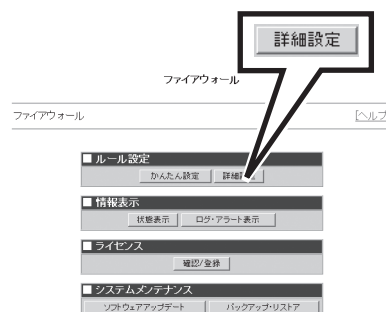
詳細設定メニューに戻る

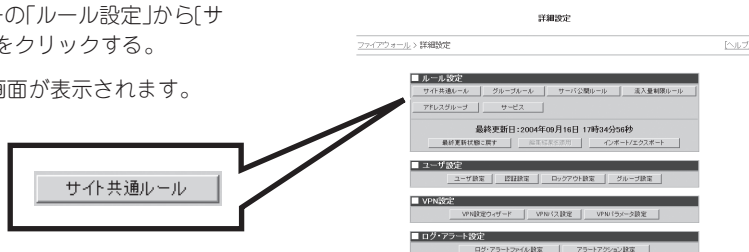
サイト共通ルールの更新

一度設定したサイト共通ルールの内容を変更することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   ルール設定一覧画面が表示されます。

詳細設定メニュー画面

4. 変更したいルールの「No.」をクリックする。

   ルール設定更新画面が表示されます。

サイト共通ルール設定一覧画面

一覧の背景がピンク色の項目は、「かんたん設定ウィザード」を経由して設定されたルールであることを示しています。このルールについては、「記録」の項目についてのみしか変更することができません。その他の項目を更新する場合は、もう一度「かんたん設定ウィザード」に戻って設定をやり直してください。

5. ルール設定更新画面に表示される各項目を設定する。

ルール設定更新画面

項　目		説　明
処理	許可	パケットを通します。
	破棄	パケットを破棄し、発信元へ応答を返しません。
	拒否	パケットを拒否し、発信元へエラーを返します。
発信元	ユーザ指定	ユーザの指定した発信元に対し処理を適用します。 テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループは、184ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークからの通信です。
	内部	内部ネットワークからの通信です。
	DMZ	DMZからの通信です。
	任意	発信元に関わらず処理を適用します。
	上記指定以外	チェックボックスをチェックすると、選択した発信元以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を発信元とする通信に対し処理を適用します。
宛先	ユーザ指定	ユーザの指定した宛先に対し処理を適用します。 テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループは、184ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークへの通信です。
	内部	内部ネットワークへの通信です。

宛先	DMZ	DMZへの通信です。
	任意	宛先に関わらず処理を適用します。
	ファイア ウォール自身	ファイアウォール自身への通信です。
	上記指定以外	チェックボックスをチェックすると、選択した宛先以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を宛先とする通信に対し処理を適用します。
通信種別	ユーザ指定	ユーザの指定したプロトコル種別に対して処理を適用します。テキストエリアにプロトコル種別を直接入力するかサービス種別をリストから指定します。サービス種別から指定する場合は、サービスのリストからサービス種別を選択し、[←]をクリックします。クリックするとテキストエリアに選択したサービスが表示されます。サービスのリストには、195ページの「サービス」で登録したものと標準定義サービスが表示されます。
	任意	通信種別に関わらず処理を適用します。
記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート	通信のログを残すとともにアラート情報も残します。

- 発信元および宛先が含むアドレスグループのメンバの数の合計は、直接入力したアドレスの数を含めて最大50個までです。
- 通信種別が含むサービスのメンバの数の合計は、直接入力した要素の数を含めて最大50個までです。

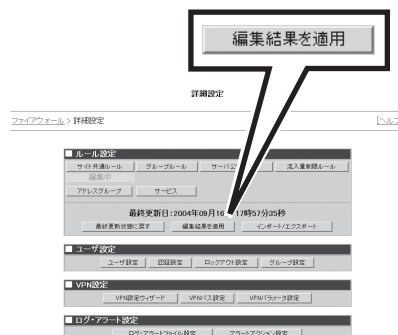
6. [登録]をクリックする。

ルール設定更新結果画面が表示されます。

チェック

登録に失敗した場合は、エラー内容を示す画面を表示します。

7. [ルール設定(サイト共通)に戻る]をクリックする。

更新したルールが反映されたルール設定一覧画面が表示されます。

ルール設定更新結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの更新前の状態に戻ります。

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

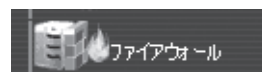
   更新したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

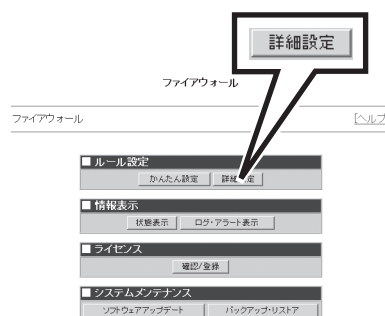
10. [詳細設定メニューに戻る]をクリックする。

ルール評価順の入れ替え

サイト共通ルールの評価順を入れ替えることができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

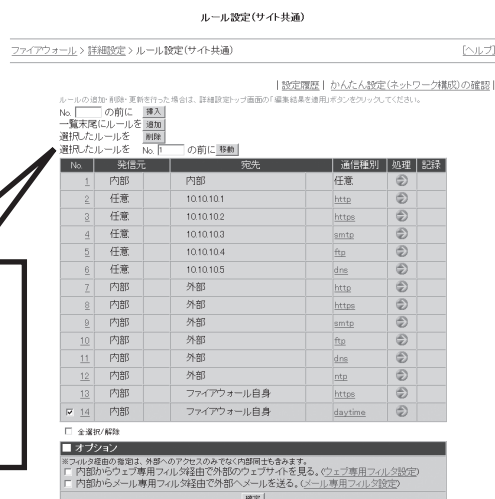
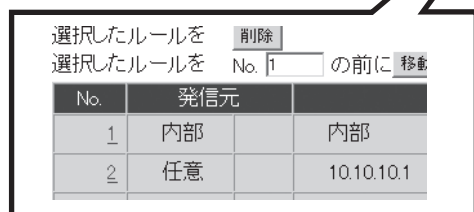
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   サイト共通ルール一覧画面が表示されます。

詳細設定メニュー画面

4. 評価順を入れ替えたいルールの「No.」の横に表示されるチェックボックスをチェックし、さらに「選択したルールをNo.の前に『移動』」の「No.」のテキストボックスにルールの番号を入力し、「選択したルールをNo.の前に『移動』」クリックする。

サイト共通ルール設定一覧画面

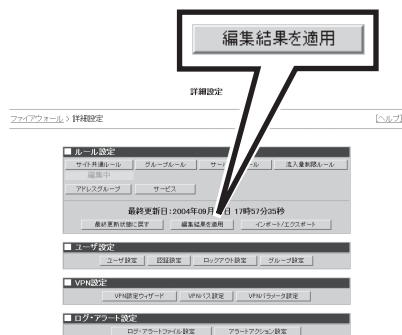
ヒント

- 「かんたん設定ウィザード」で設定されたルール(背景ピンク色)の間にもルールを移動することはできますが、再度「かんたん設定ウィザード」を用いてルールを再生成した場合、移動したルールは一覧の上部に表示され、「かんたん設定ウィザード」で設定したルールよりも評価順が上位になります。
- 「かんたん設定ウィザード」で設定されたルールよりも下位にあるルールについては、再度「かんたん設定ウィザード」を用いてルールを再生成した場合でも、評価順は下位のままです。

評価順が反映されたルール設定一覧画面が表示されます。

5. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順4で「選択したルールをNo.の前に『移動』」をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの評価順変更前の状態に戻ります。**

6. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しい評価順のサイト共通ルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

7. [詳細設定メニューに戻る]をクリックする。

内部から外部への通信におけるウェブ専用フィルタの設定

内部ネットワークまたはDMZから外部ネットワークへのHTTP通信のフィルタリング設定を行うことができます。ここでは、アクセス制御するURLを設定することで内部ネットワークから外部ネットワークへのHTTP通信を制限します。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   ルール設定一覧画面が表示されます。

詳細設定メニュー画面

4. 「オプション」の「ウェブ専用フィルタ設定」をクリックする。

ウェブ専用フィルタ設定(内→外)画面が表示されます。

ルール設定(サイト共通)

ファイアウォール > 詳細設定 > ルール設定(サイト共通) [ヘルプ]

| 設定履歴 | かんたん設定(ネットワーク構成)の確認 |

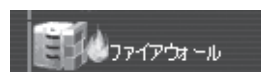
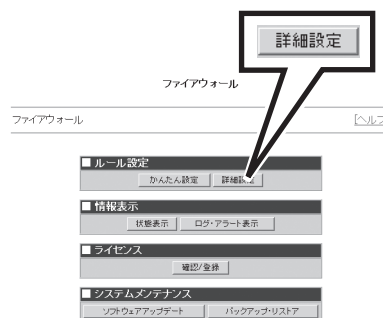
ルールの追加・削除・更新を行った場合は、詳細設定トップ画面の「編集結果を適用」ボタンをクリックしてください。

No. [ ] の前に [挿入]
一覧末尾にルールを [追加]
選択したルールを [削除]
選択したルールを No. [ ] の前に [移動]

No.	発信元		宛先		通信種別	処理	記録
1	内部		外部	以外	daytime		
2	内部		内部		任意		
3	任意		10.10.10.1		http		
4	任意		10.10.10.2		https		
5	任意		10.10.10.3		smtp		
6	任意		10.10.10.4		ftp		
7	任意		10.10.10.5		dns		
8	内部		外部		http		
9	内部		外部		https		
10	内部		外部		smtp		
11	内部		外部		ftp		
12	内部		外部		dns		
13	内部		外部		ntp		
14	内部		ファイアウォール自身		https		

全選択/解除

■ オプション

※フィルタ経由の指定は、外部へのアクセスのみでなく内部同士も含みます。
内部からウェブ専用フィルタ経由で外部のウェブサイトを見る。(ウェブ専用フィルタ設定)
内部からメール専用フィルタ経由で外部へメールを送る。(メール専用フィルタ設定)
[確定]

(ウェブ専用フィルタ設定)

サイト共通ルール設定一覧画面

5. 「アクセス禁止URL」のテキストエリアにHTTP通信を拒否したいURLを入力する。

ファイアウォール > 詳細設定 > ルール設定(サイト共通) > ウェブ専用フィルタ設定 [ヘルプ]

■ アクセス禁止URLチェックレベル説明

アクセス禁止URLチェックレベルの数値が大きくなるほど、記述したアクセス禁止URLへのアクセスを強固に禁止します。
その副作用として、アクセス禁止URLに記述していない URLへのアクセスを誤認識して禁止する可能性が高くなります。

各レベルでの、禁止規則は以下の通りです。

レベル1	アクセス禁止URLに指定されたものと前方一致するURLへのアクセスを禁止します。
レベル2	1に加え、アクセス禁止URLで指定されているホストが、複数のIPアドレス を持っている場合、そのすべてのIPアドレスを指定してのアクセスも禁止します。
レベル3	2に加え、ブラウザが接続先サーバ情報を省略(HTTP/1.0以前を使用すること で可能)し、ファイアウォールが接続先ドメイン名を取得できなかった場 合も禁止します。
レベル4	3に加え、Proxyのトンネル機能を利用したアクセスすべてを禁止します。

ウェブ専用フィルタ設定(内→外)画面

ヒント

- 1行につき1つのURLを指定してください。URLとして最大で1000バイトまでの文字列を指定できます。
- URLの記述は、「http://」から始め、パス部分まで設定することができます。
  ただし、パスごとに設定する必要はなく、指定した文字列で始まるURLはすべてアクセス制御がかかります。たとえば、「http://web.server.name/data1/」と指定すると、「http://web.server.name/data1/data2/」などもアクセス禁止になります。
- URLの一部として、「＊」が利用できます。たとえば「web*.server.name」というように指定することもできます。

この機能の対象ポートは、HTTP(ポート番号80)です。独自のポート番号で公開していたり、セキュリティで保護されている(https)ウェブサーバには使用できません。

6. アクセス禁止URLチェックレベルをプルダウンメニューより選択する。

   アクセス禁止レベルは数値が大きくなるほど、設定したURLへのアクセス制御を強固にします。アクセスレベルの詳細については、画面に表示される内容を確認してください。

7. ［設定］をクリックする。

   ウェブ専用フィルタ設定（内→外）結果画面が表示されます。

■ アクセス禁止URLチェックレベル説明

アクセス禁止URLチェックレベルの数値が大きくなるほど、記述したアクセス禁止URLへのアクセスを強固に禁止します。
その副作用として、アクセス禁止URLに記述していない URLへのアクセスを誤認識して禁止する可能性が高くなります。

各レベルでの、禁止規則は以下の通りです。

レベル1	アクセス禁止URLに指定されたものと前方一致するURLへのアクセスを禁止します。
レベル2	1に加え、アクセス禁止URLで指定されているホストが、複数のIPアドレス を持っている場合、そのすべてのIPアドレスを指定してのアクセスも禁止します。
レベル3	2に加え、ブラウザが接続先サーバ情報を省略(HTTP/1.0以前を使用することで可能)し、ファイアウォールが接続先ドメイン名を取得できなかった場 合も禁止します。
レベル4	3に加え、Proxyのトンネル機能を利用したアクセスすべてを禁止します。

ウェブ専用フィルタ設定（内→外）画面

8. ［ルール設定（サイト共通）に戻る］をクリックする。

   サイト共通ルール一覧画面が表示されます。

ウェブ専用フィルタ設定（内→外）結果画面

9. 「内部からウェブ専用フィルタ経由で外部のウェブサイトを見る。」のチェックボックスにチェックし、［確定］をクリックする。

   設定結果画面が表示されるので、［ルール設定（サイト共通）に戻る］をクリックします。

ルール設定(サイト共通)

ファイアウォール > 詳細設定 > ルール設定(サイト共通) [ヘルプ]

| 設定履歴 | かんたん設定(ネットワーク構成)の確認 |

ルールの追加・削除・更新を行った場合は、詳細設定トップ画面の「編集結果を適用」ボタンをクリックしてください。

No. の前に 挿入
一覧末尾にルールを 追加
選択したルールを 削除
選択したルールを No. の前に 移動

No.	発信元		宛先		通信種別	処理	記録
1	内部		外部	以外	daytime		
2	内部		内部		任意		
3	任意		10.10.10.1		http		
4	任意		10.10.10.2		https		
5	任意		10.10.10.3		smtp		
6	任意		10.10.10.4		ftp		
7	任意		10.10.10.5		dns		
8	内部		外部		http		
9	内部		外部		https		
10	内部		外部		smtp		
11	内部		外部		ftp		
12	内部		外部		dns		
13	内部		外部		ntp		
14	内部		ファイアウォール自身		https		

全選択/解除

サイト共通ルール設定一覧画面

重要

［確定］をクリックしないと、ウェブ専用フィルタ設定をしてもフィルタリング機能は有効になりません。逆にウェブ専用フィルタ設定をしないでフィルタリング機能を有効にしても効果はありません。

10. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順9で[確定]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はフィルタリング機能の設定前の状態に戻ります。**

11. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

フィルタリング設定がExpress5800/SG300に適用され、設定結果画面が表示されます。

12. [詳細設定メニューに戻る]をクリックする。

詳細設定

ファイアウォール > 詳細設定 > 設定結果

新しいルールを適用しました。

詳細設定メニューに戻る

内部から外部への通信におけるメール専用フィルタの設定

内部ネットワークから外部ネットワークへのSMTP通信のフィルタリング設定を行うことができます。SMTP通信のフィルタリングでは、内部ネットワークから外部ネットワークへのSMTP通信において、内部ネットワーク内の端末のIPアドレスを隠蔽します。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   ルール設定一覧画面が表示されます。

詳細設定メニュー画面

ファイアウォール機能の設定方法

4. 「オプション」の「メール専用フィルタ設定」をクリックする。

   メール専用フィルタ設定(内→外)画面が表示されます。

サイト共通ルール設定一覧画面

5. 内部IPアドレス隠蔽機能の利用の有無を選択する。

   - する
     内部IPアドレス隠蔽機能を利用する場合、このラジオボタンをクリックします。
   - しない
     内部IPアドレス隠蔽機能を利用しない場合、このラジオボタンをクリックします。

メール専用フィルタ設定(内→外)画面

この機能の対象ポートは、SMTP(ポート番号25)です。独自のポート番号で公開しているメールサーバには使用できません。

6. [設定]をクリックする。

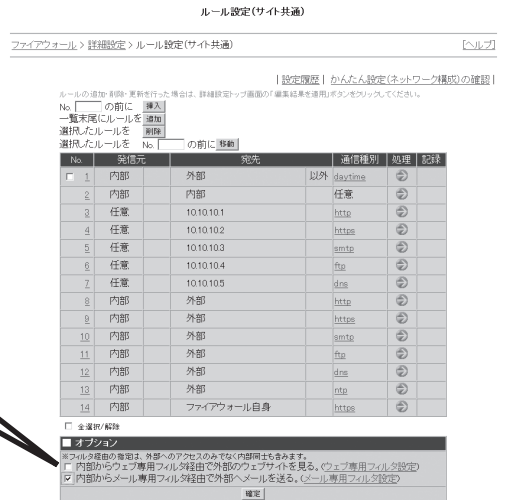
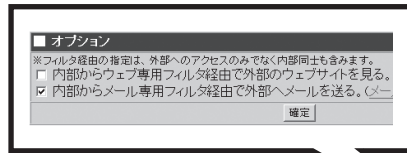
   メール専用フィルタ設定(内→外)結果画面が表示されます。

7. [ルール設定(サイト共通)に戻る]をクリックする。

   サイト共通ルール一覧画面が表示されます。

メール専用フィルタ設定(内→外)結果画面

8. 「内部からメール専用フィルタ経由で外部へメールを送る。」のチェックボックスにチェックし、[確定]をクリックする。

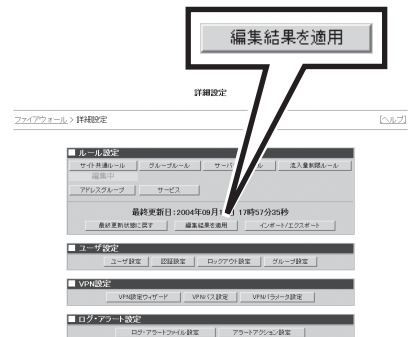
   設定結果画面が表示されるので、[ルール設定(サイト共通)に戻る]をクリックします。

サイト共通ルール設定一覧画面

重要

[確定]をクリックしないと、メール専用フィルタ設定をしてもフィルタリング機能は有効になりません。逆にメール専用フィルタ設定をしないでフィルタリング機能を有効にしても効果はありません。

9. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順8で[確定]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はフィルタリング機能の設定前の状態に戻ります。**

10. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

    フィルタリング設定がExpress5800/SG300に適用され、設定結果画面が表示されます。

11. [詳細設定メニューに戻る]をクリックする。

グループルール

グループルールとは、グループに所属するユーザが認証を行うことで適用されるルールのことです。ここでは、サイト共通ルールでの設定に対し、グループ単位で例外的に許可するルールを設定します。たとえば、以下のような設定ができます。

- サイト共通ルールではHTTP通信を拒否するが、ある部署に所属するメンバだけには、指定する端末へのHTTP通信を許可する
- サイト共通ルールではサーバへのアクセスを拒否するが、プロジェクトメンバに対してだけは、プロジェクトで利用するサーバへのアクセスを許可する

Express5800/SG300は、ユーザの所属しているグループのルールに従って通信の種別や宛先から通信の許可、アクセスログの取得などの処理を判断します。ユーザが所属するグループルールにおいては上位に表示されるものから順番に評価を行います。

ユーザ認証実行後、有効時間内は所属しているグループルールが適用されます。有効時間内を過ぎてから、ユーザがグループルールで許可されたExpress5800/SG300を超える通信を行う場合は、再度ログインする必要があります。

グループルールでは、以下のような設定・管理を行うことができます。

- グループルールの設定内容の確認
- グループルールの追加
- グループルールの削除
- グループルールの更新

あらかじめグループの設定を行っていないとグループルールの設定・管理を行うことはできません。グループの設定については、235ページの「グループ設定」を参照してください。

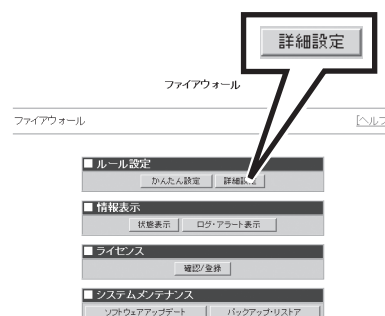
グループルールの設定内容の確認

すでに設定したルールはグループルール一覧画面から確認することができます。

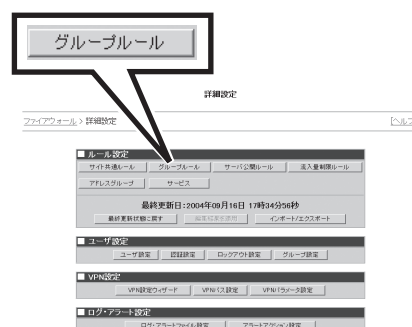
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[グループルール]をクリックする。

   グループルール一覧画面が表示されます。表示される内容は以下の通りです。

詳細設定メニュー画面

項　目	説　明
グループ番号	[001]のような形式でシステムがグループに付与した番号が表示されます。
グループ名	グループ名です。
認証有効時間	ユーザ認証後グループルールが適用される有効時間です。
トランスポートVPNパス	VPNパスを使用するかどうかを表示します。
No.	ルールの番号です。通信を通すか否かの判定の際は、番号の若いルールから順番に評価した結果、最初にマッチしたルールに基づいて処理されます。
発信元	「ユーザが使用中のホスト」です。
宛先	パケットの宛先を表すIPアドレス、ネットワークアドレス、あるいは内部、外部、DMZ、任意、ファイアウォール自身、指定した宛先以外のいずれかです。

項　目	説　明	
通信種別	パケットのプロトコル種別を表します。	
処理		パケットを通します。
記録		通信のログを残します。
		通信のログを残すとともにアラート情報も残します。
	［空白］	ログもアラートも残しません。

グループルール一覧画面

ヒント

画面右上の「かんたん設定(ネットワーク構成)の確認」をクリックすると、かんたん設定で設定した内容が別ウィンドウで表示されます。

上記の画面を例にして具体的なグループルール一覧の事例を示します。

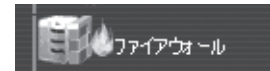
[001]のグループルールでは、group2に所属するユーザはExpress5800/SG300上での認証に成功すると、以下のルールが適用されます。認証の有効時間は60分です。

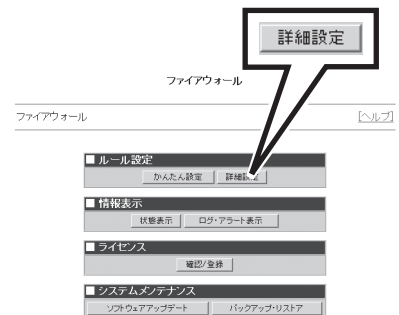
ルールの1行目:　ユーザの端末と内部ネットワークにある端末間のすべての通信を許可することを表します。

ルールの2行目:　ユーザの端末から外部ネットワークへのHTTP通信を許可することを表します。

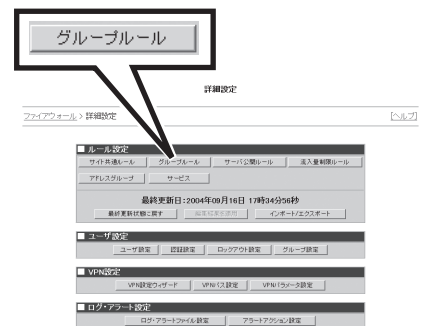
グループルールの追加

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

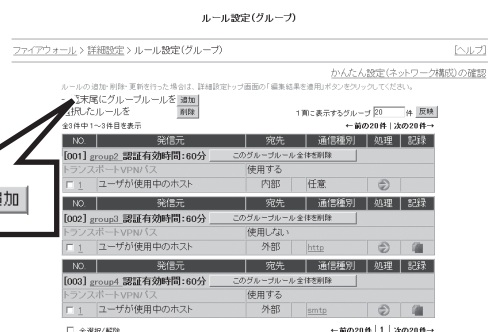
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

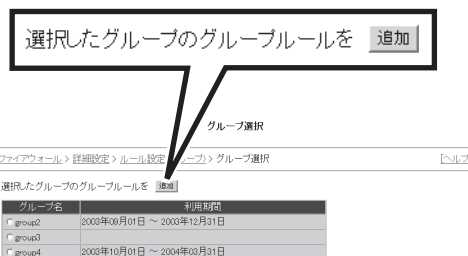
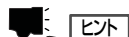
3. 詳細設定メニューの「ルール設定」から[グループルール]をクリックする。

   グループルール一覧画面が表示されます。

詳細設定メニュー画面

4. 「一覧末尾にグループルールを『追加』」をクリックする。

   グループ選択画面が表示されます。

グループルール一覧画面

5. ルールを追加するグループ名のラジオボタンをクリックし、「選択したグループのグループルールを『追加』」をクリックする。

   選択したグループのルール一覧画面が表示されます。

グループ選択画面

> **ヒント**
>
> グループルールの一覧画面からグループ名をクリックすることでも、選択したグループのルール一覧画面を表示することができます。

6. 「認証有効時間」のテキストボックスに、ユーザ認証の後、ルールを有効にしておく時間を分単位で入力する。

グループルール

ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール [ヘルプ]

group3

■ 認証有効時間

60 分

一覧末尾に 追加

選択したルールを 削除

No.	発信元	宛先	通信種別	処理	記録
1	ユーザが使用中のホスト	外部	http		

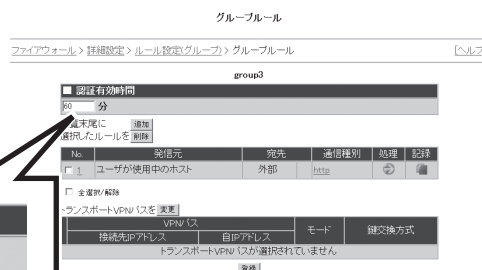
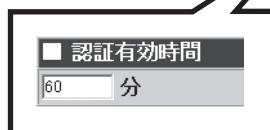
全選択/解除

トランスポートVPNパスを 変更

VPNパス		モード	鍵交換方式
接続先IPアドレス	自IPアドレス		
トランスポートVPNパスが選択されていません			

登録

■ 認証有効時間

60 分

選択したグループのルール一覧画面

> **ヒント**
>
> 設定した有効期限を過ぎてから、ユーザがグループルールで許可されたExpress5800/SG300を超える通信を行う場合は、再度ログインする必要があります。

7. ある特定のアドレスから通信を行う際にVPNを利用する場合は、「トランスポートVPNパスを『変更』」をクリックする。

   VPNを利用しない場合は、手順9に進んでください。

   トランスポートVPNパス選択画面が表示されます。

グループルール

ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール [ヘルプ]

group3

■ 認証有効時間

60 分

一覧末尾に 追加

選択したルールを 削除

No.	発信元	宛先	通信種別	処理	記録
1	ユーザが使用中のホスト	外部	http		

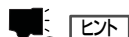
全選択/解除

トランスポートVPNパスを 変更

VPNパス		モード	鍵交換方式
接続先IPアドレス	自IPアドレス		
トランスポートVPNパスが選択されていません			

登録

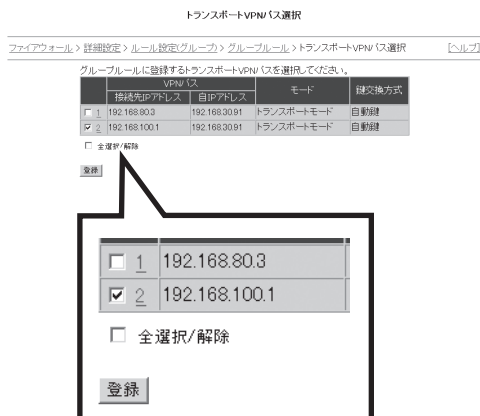
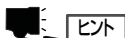
トランスポートVPNパスを 変更

選択したグループのルール一覧画面

> **ヒント**
>
> トランスポートVPNパスはあらかじめVPNパスを設定していないと表示されません。トランスポートVPNパスの設定については、244ページの「VPN設定」を参照してください。

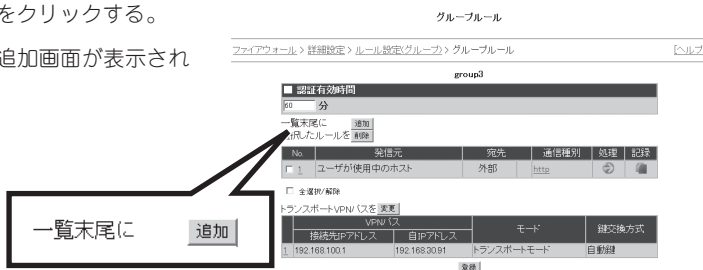
8. 表示されるトランスポートVPNパスの中から利用するVPNパスのチェックボックスをチェックし、［登録］をクリックする。

選択したグループルールの一覧画面に戻ります。引き続き、グループルールの設定を行う場合は、手順9に進みます。ここでグループルールの設定を終了する場合は、手順13に進みます。

トランスポートVPNパス選択画面

ヒント

選択したグループのルール一覧画面で、追加したVPNパスの番号をクリックすると、そのVPNパスの詳細設定を確認することができます。

9. 「一覧末尾に『追加』」をクリックする。

グループルール設定追加画面が表示されます。

選択したグループのルール一覧画面

10. グループルール設定追加画面に表示される各項目を設定する。

項　目		説　明
処理	許可	パケットを通します。設定の変更はできません。
発信元	ユーザが使用中のホスト	ユーザが使用している端末を発信元とする通信にルールを適用します。設定の変更はできません。
宛先	ユーザ指定	ユーザの指定した宛先に対し処理を適用します。テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、［←］をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループのリストには、184ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークへの通信です。
	内部	内部ネットワークへの通信です。
	DMZ	DMZへの通信です。
	任意	宛先に関わらず処理を適用します。
	ファイアウォール自身	ファイアウォール自身への通信です。
	上記指定以外	チェックボックスをチェックすると、選択した宛先以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を宛先とする通信に対し処理を適用します。

項　目		説　明
通信種別	ユーザ指定	ユーザの指定したプロトコル種別に対して処理を適用します。テキストエリアにプロトコル種別を直接入力するかサービス種別をリストから指定します。サービス種別から指定する場合は、サービスのリストからサービス種別を選択し、[←]をクリックします。クリックするとテキストエリアに選択したサービスが挿入されます。サービスのリストには、195ページの「サービス」で登録したものと標準定義サービスが表示されます。
	任意	通信種別に関わらず処理を適用します。
記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート	通信のログを残すとともにアラート情報も残します。

ヒント

- 宛先が含むアドレスグループのメンバの数の合計は、直接入力したアドレスの数を含めて最大50個までです。
- 通信種別が含むサービスのメンバの数の合計は、直接入力した要素の数を含めて最大50個までです。

グループルール設定追加画面

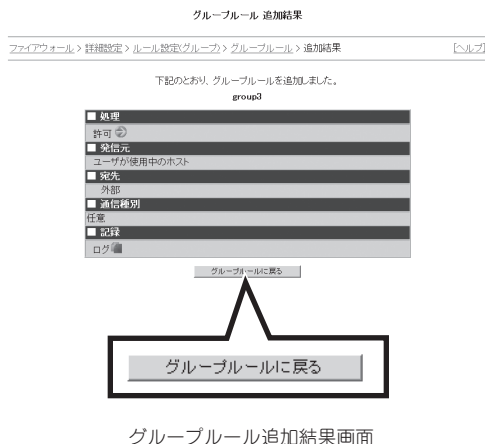
11. [登録]をクリックする。

グループルール追加結果画面が表示されます。

グループルールの登録に失敗した場合は、エラー内容を示す画面が表示されます。

12. ［グループルールに戻る］をクリックする。

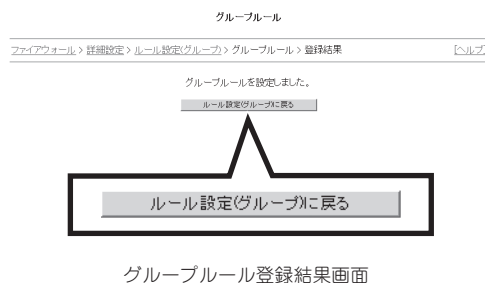
追加したルールが反映された、選択したグループのルール一覧画面が表示されます。

グループルール追加結果画面

13. ［登録］をクリックする。

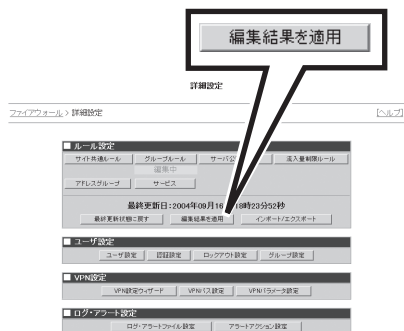
グループルール登録結果画面が表示されます。

選択したグループのルール一覧画面

14. ［ルール設定(グループ)に戻る］をクリックする。

グループルール登録結果画面

15. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順11で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの追加前の状態に戻ります。

16. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

新しく追加したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

17. [詳細設定メニューに戻る]をクリックする。

詳細設定

ファイアウォール > 詳細設定 > 設定結果

新しいルールを適用しました。

詳細設定メニューに戻る

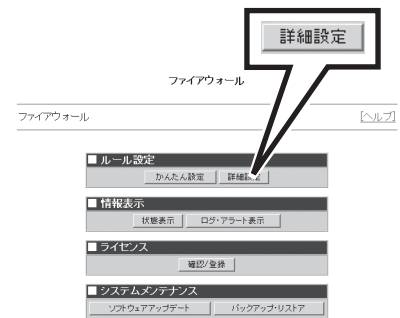
グループルールの削除

設定したグループルールを削除することができます。

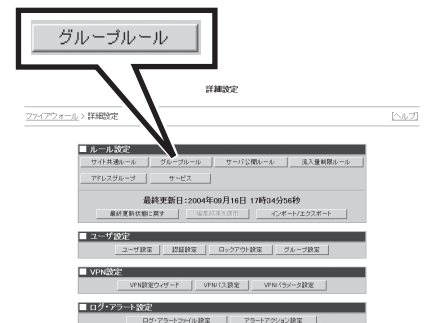
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

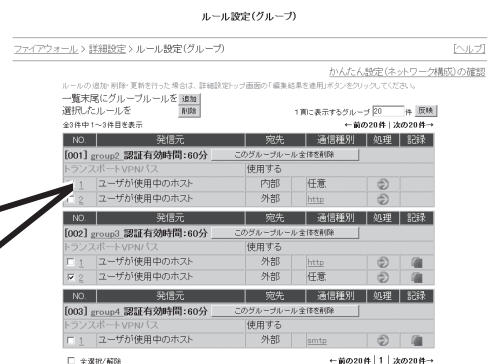
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[グループルール]をクリックする。

   グループルール一覧画面が表示されます。

詳細設定メニュー画面

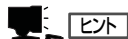
4. 削除したいルールの「No.」の横に表示されているチェックボックスをチェックし、「選択したルールを『削除』」をクリックする。

グループルール一覧画面

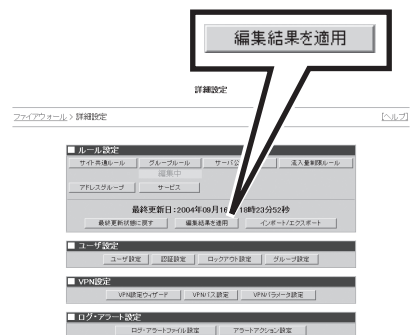
ヒント

- 「全選択/解除」のチェックボックスをチェックすると、削除可能なルールのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのルールを削除対象から外すこともできます。
- グループルール一覧からグループ名をクリックし、選択したグループのルール一覧画面からルールを削除することもできます。
- [このグループルール全体を削除]をクリックすると、選択したグループのグループルールがすべて削除されます。

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

   グループルールが削除され、ルールが削除されたグループルール一覧画面が表示されます。

ヒント

[キャンセル]をクリックすると、削除されずにグループルール一覧画面に戻ります。

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階ではルールの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの削除前の状態に戻ります。**

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

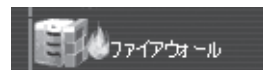
   ルールの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

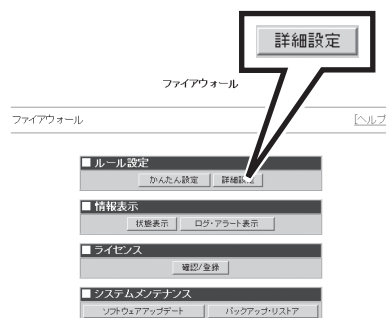
8. [詳細設定メニューに戻る]をクリックする。

グループルールの更新

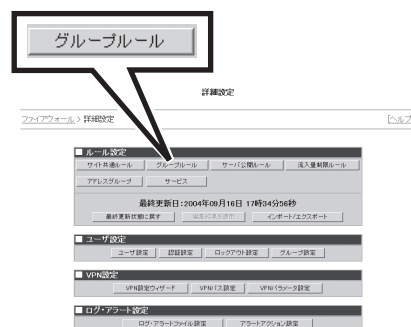
一度設定したグループルールの内容を変更することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

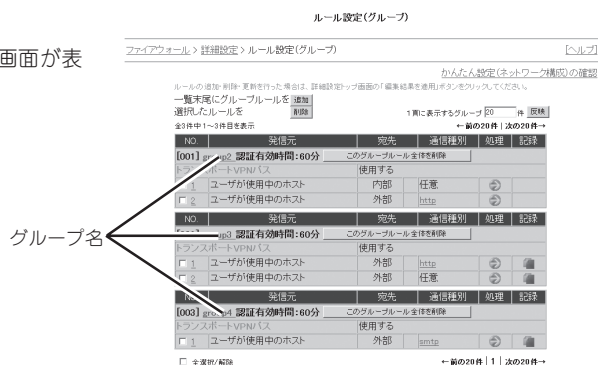
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[グループルール]をクリックする。

   グループルール一覧画面が表示されます。

詳細設定メニュー画面

4. グループ名をクリックする。

   選択したグループのルール一覧画面が表示されます。

グループルール一覧画面

5. 変更したいルールの「No.」をクリックする。

グループルール設定更新画面が表示されます。

選択したグループのルール一覧画面

6. グループルール設定更新画面に表示される各項目を設定する。

項　目		説　明
処理	許可	パケットを通します。設定の変更はできません。
発信元	ユーザが使用中のホスト	ユーザが使用している端末を発信元とする通信にルールを適用します。設定の変更はできません。
宛先	ユーザ指定	ユーザの指定した宛先に対し処理を適用します。テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループのリストには、184ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークへの通信です。
	内部	内部ネットワークへの通信です。
	DMZ	DMZへの通信です。
	任意	宛先に関わらず処理を適用します。
	ファイアウォール自身	ファイアウォール自身への通信です。
	上記指定以外	チェックボックスをチェックすると、選択した宛先以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を宛先とする通信に対し処理を適用します。
通信種別	ユーザ指定	ユーザの指定したプロトコル種別に対して処理を適用します。テキストエリアにプロトコル種別を直接入力するかサービス種別をリストから指定します。サービス種別から指定する場合は、サービスのリストからサービス種別を選択し、[←]をクリックします。クリックするとテキストエリアに選択したサービスが挿入されます。サービスのリストには、195ページの「サービス」で登録したものと標準定義サービスが表示されます。
	任意	通信種別に関わらず処理を適用します。
記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート	通信のログを残すとともにアラート情報も残します。

- 宛先が含むアドレスグループのメンバの数の合計は、直接入力したアドレスの数を含めて最大50個までです。
- 通信種別が含むサービスのメンバの数の合計は、直接入力した要素の数を含めて最大50個までです。

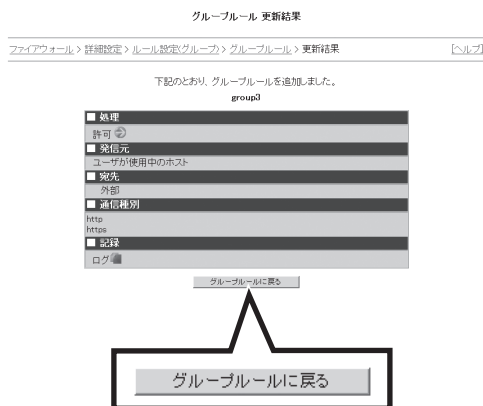
7. ［登録］をクリックする。

   グループルール更新結果画面が表示されます。

グループルールの更新に失敗した場合はエラー内容を示す画面が表示されます。

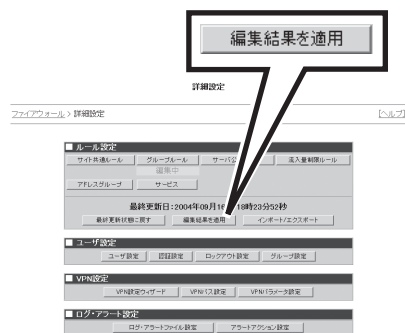
グループルール設定更新画面

8. ［グループルールに戻る］をクリックする。

   更新したルールが反映された選択したグループのルール一覧画面が表示されま

グループルール更新結果画面

9. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順7で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの更新前の状態に戻ります。

10. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

    更新したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

11. [詳細設定メニューに戻る]をクリックする。

サーバ公開ルール

サーバ公開ルールとは、Express5800/SG300を導入した環境において、DMZまたは、内部ネットワーク上にあるサーバを外部ネットワークに公開する際に、アドレス変換(NAT)およびウェブ/メール専用フィルタの制御を行うためのルールのことです。
サーバ公開ルールでは、以下のような設定・管理を行うことができます。

- サーバ公開ルールの設定内容の確認
- サーバ公開ルールの追加
- サーバ公開ルールの削除
- サーバ公開ルールの更新
- 外部から内部への通信におけるウェブ専用フィルタの設定
- 外部から内部への通信におけるメール専用フィルタの設定

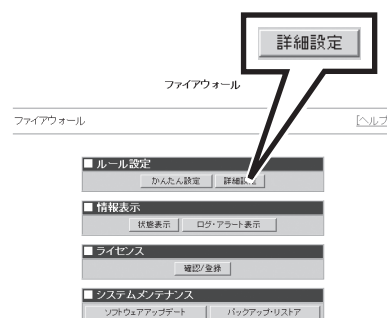
サーバ公開ルールの設定内容の確認

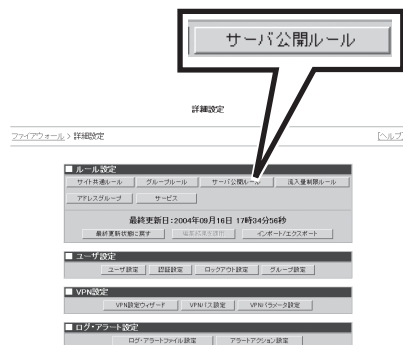
かんたん設定ウィザードから設定したサーバ公開ルールや、すでに設定したルールはサーバ公開ルール一覧画面から確認することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から［サーバ公開ルール］をクリックする。

詳細設定メニュー画面

サーバ公開ルール一覧画面が表示されます。表示される内容は以下の通りです。

<table>
<tr><th>項　目</th><th colspan="2">説　明</th></tr>
<tr><td>公開IPアドレス</td><td colspan="2">外部ネットワークへ公開するサーバのIPアドレスです。</td></tr>
<tr><td>ポート</td><td colspan="2">外部ネットワークへ公開するサーバのポート番号です。</td></tr>
<tr><td>内部IPアドレス</td><td colspan="2">内部ネットワークでのサーバのIPアドレスです。</td></tr>
<tr><td>ポート</td><td colspan="2">内部ネットワークでのサーバのポート番号です。</td></tr>
<tr><td rowspan="2">記録</td><td></td><td>通信のログを残します。</td></tr>
<tr><td>〔空白〕</td><td>ログもアラートも残しません。</td></tr>
</table>

サーバ公開ルール一覧画面

- 画面右上の「かんたん設定(ネットワーク構成)の確認」をクリックすると、かんたん設定で設定した内容が別ウィンドウで表示されます。
- 内部ネットワーク上の端末のアドレスをすべて本ファイアウォールのアドレスで置き換える機能(NAPT)は、かんたん設定のインタフェースの選択画面から設定します。

重要

- この画面でサーバ公開の設定をしても、アクセス許可はされません。サーバへのアクセス許可についてはサイト共通ルール画面からルールを設定する必要があります。サイト共通ルール設定の際は、公開IPアドレスではなく、内部IPアドレスで設定してください。
- Express5800/SG300の外部インタフェースのIPアドレスを公開アドレスとして使用することもできますが、公開するポート番号がユーザ認証ウェブ(112ページ参照)と重複しないよう注意してください。
- メール専用フィルタ設定やウェブ専用フィルタ設定、不正アクセス対策(アドバンスレベル)設定は、サーバ公開ルールに従ってアクセス制限を行います。

  外部ネットワークからアクセスするウェブサーバやメールサーバは、すべて登録してください。

具体的なサーバ公開ルール一覧の事例を示します。

No.	公開IPアドレス	ポート	内部IPアドレス	ポート	記録
1	192.168.30.1	tcp/443	192.168.20.1	443	
2	192.168.30.1	tcp/25	192.168.20.1	25	
□ 3	192.168.30.5	全部	192.168.20.2	全部	
□ 4	192.168.30.40	全部	192.168.20.10	全部	

サーバ公開ルール一覧画面

ルールの1行目: 内部アドレス192.168.20.1の端末がTCPポート443番で待ち受けているサービスを、外部ネットワークへIPアドレス192.168.30.1、TCPポート443番で公開することを示しています。

ルールの2行目: 内部アドレス192.168.20.1の端末がTCPポート25番で待ち受けているサービスを、外部ネットワークへIPアドレス192.168.30.1、TCPポート25番で公開することを示しています。

ルールの3行目: 内部アドレス192.168.20.2の端末が待ち受けているサービスを、外部ネットワークへIPアドレス192.168.30.5で公開することを示しています。

ルールの4行目: 内部アドレス192.168.20.10の端末が待ち受けているサービスを、外部ネットワークへIPアドレス192.168.30.40で公開することを示しています。

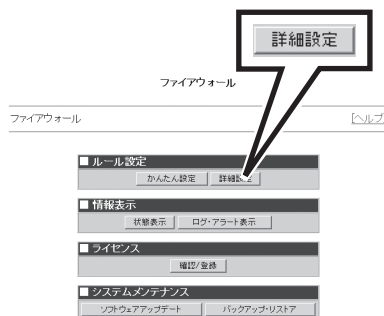
サーバ公開ルールの追加

必要に応じてサーバ公開ルールを追加することができます。

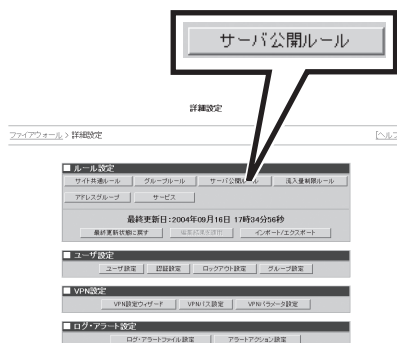
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。

詳細設定メニュー画面

4. 「一覧末尾にルールを『追加』」をクリックする。

   ルール設定追加画面が表示されます。

サーバ公開ルール一覧画面

5. ルール設定追加画面に表示される各項目を入力する。

   - 外部公開IPアドレス
     外部ネットワークへ公開するIPアドレスを入力します。
   - 内部IPアドレス
     サーバの実際のIPアドレスを指定します。「外部公開IPアドレス」と異なる場合は、そのIPアドレスを入力します。「外部公開IPアドレス」と同じ場合は、「アドレス変換しない」をクリックします。
   - ポート
     ポート番号の指定を行うかどうかを選択します。特定のポート番号についてのみ公開するか、ポート番号の変換を行う場合には、外部ネットワークへ公開するポート番号と、対応する内部ネットワークのポート番号を入力します。
   - 記録
     作成するルールに該当する通信パケットを検出したとき、ログ情報としてのみファイルに出力するか、それともファイルにはいっさい記録しないかを設定します。

ファイアウォール > 詳細設定 > ルール設定(サーバ公開) > ルール設定追加 [ヘルプ]

ルール設定追加画面

6. ［登録］をクリックする。

   ルール設定追加結果画面が表示されます。

7. ［ルール設定（サーバ公開）に戻る］をクリックする。

   追加したルールが反映されたサーバ公開ルール一覧画面が表示されます。

ルール設定追加結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの追加前の状態に戻ります。**

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しく追加したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

11. [詳細設定メニューに戻る]をクリックする。

サーバ公開ルールの削除

不要になったサーバ公開ルールを削除することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

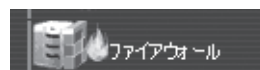
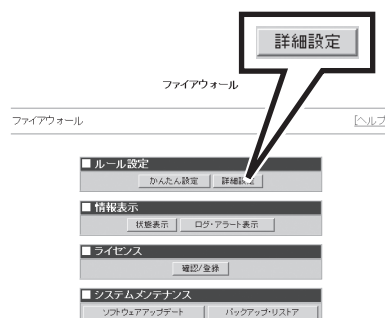
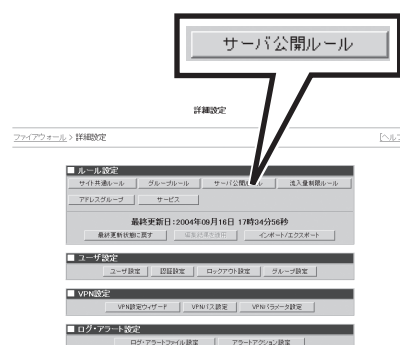
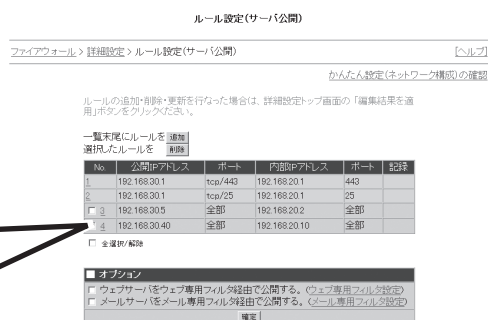
ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。

詳細設定メニュー画面

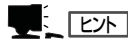
4. 削除したいルールの「No.」の横に表示されるチェックボックスをチェックし、「選択したルールを『削除』」をクリックする。

No.	公開IPアドレス
1	192.168.30.1
2	192.168.30.1
☐ 3	192.168.30.5
☑ 4	192.168.30.40

サーバ公開ルール一覧画面

ヒント

- 一覧の背景がピンク色の項目は、「かんたん設定ウィザード」を経由して設定されたルールであることを示しています。このルールについては、サーバ公開ルールの設定から削除することはできません。
- 「全選択/解除」のチェックボックスをチェックすると、削除可能なルールのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのルールを削除対象から外すこともできます。

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

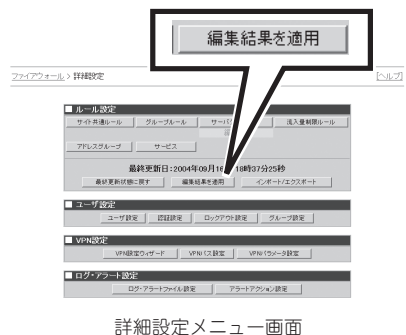
ヒント

[キャンセル]をクリックすると、削除されずにサーバ公開ルール一覧画面に戻ります。

ルールが削除されたサーバ公開ルール一覧画面が表示されます。

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順5で[OK]をクリックしますが、この段階ではルールの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの削除前の状態に戻ります。**

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

ルールの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。

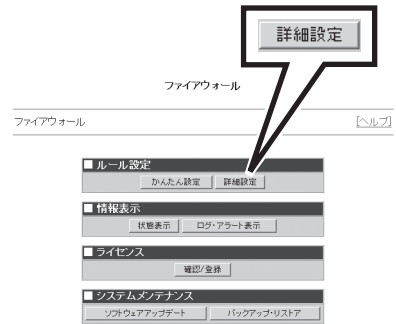
サーバ公開ルールの更新

一度設定したサーバ公開ルールの内容を変更することができます。

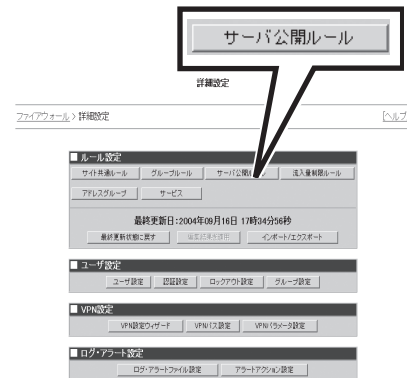
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

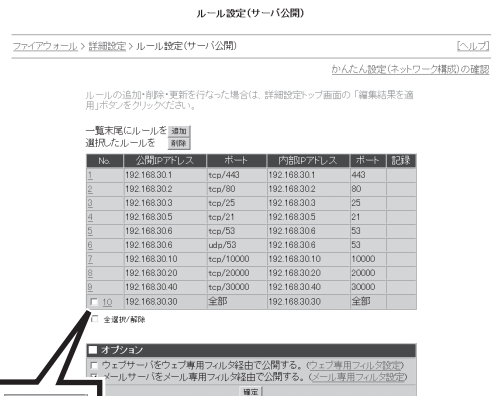
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

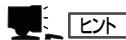
   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。

詳細設定メニュー画面

4. 変更したいルールの「No.」をクリックする。

   ルール設定更新画面が表示されます。

   一覧の背景がピンク色の項目は、「かんたん設定ウィザード」を経由して設定されたルールであることを示しています。このルールについては、「記録」の項目についてのみしか変更することができません。その他の項目を更新する場合は、もう一度「かんたん設定ウィザード」に戻って設定をやり直してください。

サーバ公開ルール一覧画面

5. ルール設定更新画面に表示される各項目を入力する。

- 外部公開IPアドレス
  外部ネットワークへ公開するIPアドレスを入力します。
- 内部IPアドレス
  サーバの実際のIPアドレスを指定します。「外部公開IPアドレス」と異なる場合は、そのIPアドレスを入力します。
- ポート
  ポート番号の指定を行うかどうかを選択します。特定のポート番号についてのみ公開するか、ポート番号の変換を行う場合には、外部ネットワークへ公開するポート番号と、対応する内部ネットワークのポート番号を入力します。
- 記録
  作成するルールに該当する通信パケットを検出したとき、ログ情報としてのみファイルに出力するか、それともファイルにはいっさい記録しないかを設定します。

ルール設定更新画面

6. ［登録］をクリックする。

ルール設定更新結果画面が表示されます。

7. ［ルール設定（サーバ公開）に戻る］をクリックする。

変更したルールが反映されたサーバ公開ルール一覧画面が表示されます。

ルール設定更新結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの更新前の状態に戻ります。

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   更新したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。

ファイアウォール機能の設定方法

外部から内部への通信におけるウェブ専用フィルタの設定

外部ネットワークから内部ネットワークへのHTTP通信のフィルタリング設定を行うことができます。ここでは、アクセス制御する端末やネットワークを設定することで外部ネットワークから内部ネットワークへのHTTP通信を制限します。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

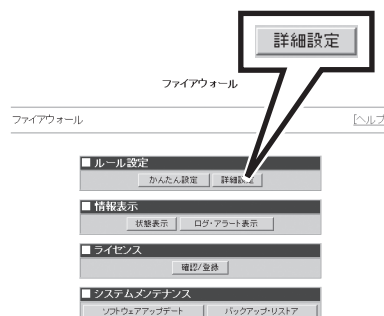
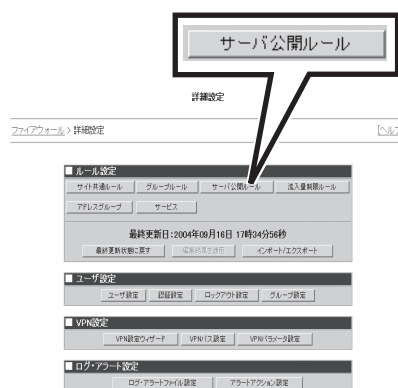
3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。

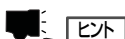
詳細設定メニュー画面

4. 「オプション」の「ウェブ専用フィルタ設定」をクリックする。

   ウェブ専用フィルタ設定(外→内)画面が表示されます。

No.	公開IPアドレス	ポート	内部IPアドレス	ポート	記録
1	192.168.30.1	tcp/443	192.168.20.1	443	
2	192.168.30.1	tcp/25	192.168.20.1	25	
3	192.168.30.5	全部	192.168.20.2	全部	
4	192.168.30.40	全部	192.168.20.10	全部	

サーバ公開ルール一覧画面

5. 一時遮断機能の利用の有無を選択する。利用する場合は、単位時間、アクセス数、遮断時間を設定する。

ウェブ専用フィルタ設定(外→内)画面

> ヒント
>
> 一時遮断機能によって、外部ネットワークの特定の端末から内部ネットワーク上のウェブサーバに過剰アクセスする攻撃(DoS攻撃)を回避します。指定する単位時間あたり、指定するアクセス数を越えて接続した場合、その送信元からのウェブアクセスを指定した遮断時間の間制限します。
>
> さらに、一時遮断機能を有効にしていると、外部ネットワークの過剰な数の端末から内部ネットワーク上のウェブサーバにアクセスする攻撃(DDoS攻撃)についても回避します。この場合は指定する単位時間あたり、50を超える送信元からのウェブアクセスを制限します。

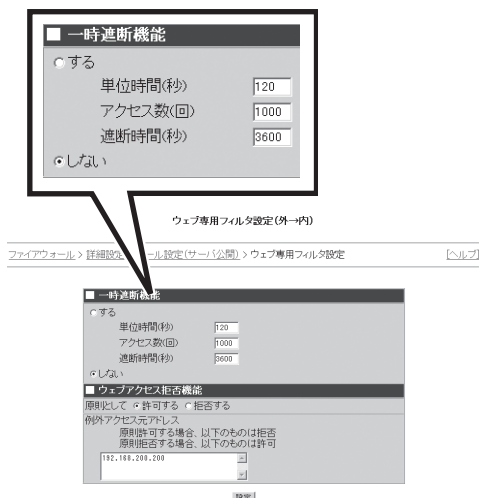
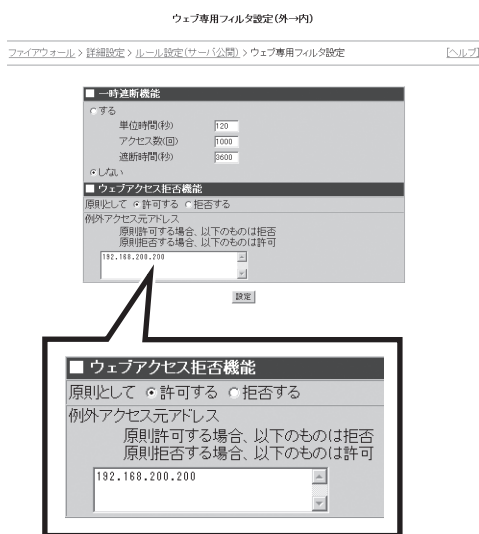
6. ウェブアクセス拒否機能を設定する。

- 原則として許可する
  ウェブサーバに対するアクセスを原則として許可する場合に選択します。例外として拒否するネットワーク、端末がある場合は、下に表示されるテキストエリアに拒否対象となるネットワークアドレスまたはIPアドレスを設定します。

- 原則として拒否する
  ウェブサーバに対するアクセスを原則として拒否する場合に選択します。例外として許可するネットワーク、端末がある場合は、下に表示されるテキストエリアに許可対象となるネットワークアドレスまたはIPアドレスを設定します。

ウェブ専用フィルタ設定(外→内)画面

7. [設定]をクリックする。

   ウェブ専用フィルタ設定(外→内)結果画面が表示されます。

8. ［ルール設定（サーバ公開）に戻る］をクリックする。

   サーバ公開ルール一覧画面が表示されます。

ウェブ専用フィルタ設定（外→内）結果画面

9. 「ウェブサーバをウェブ専用フィルタ経由で公開する。」のチェックボックスにチェックし、［確定］をクリックする。

   設定更新結果画面が表示されるので、［ルール設定（サーバ公開）に戻る］をクリックします。

サーバ公開ルール一覧画面

重要

確定をクリックしないと、ウェブ専用フィルタ設定をしてもフィルタリング機能は有効になりません。逆にウェブ専用フィルタ設定をしないでフィルタリング機能を有効にしても効果はありません。

10. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順9で［確定］をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには［編集結果を適用］をクリックしてください。**
- **［最終更新状態に戻す］をクリックすると、Express5800/SG300はフィルタリング機能の設定前の状態に戻ります。**

11. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

    フィルタリング設定がExpress5800/SG300に適用され、設定結果画面が表示されます。

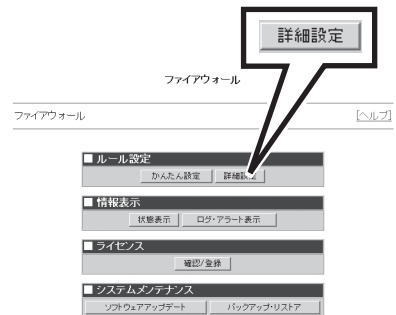
12. ［詳細設定メニューに戻る］をクリックする。

外部から内部への通信におけるメール専用フィルタの設定

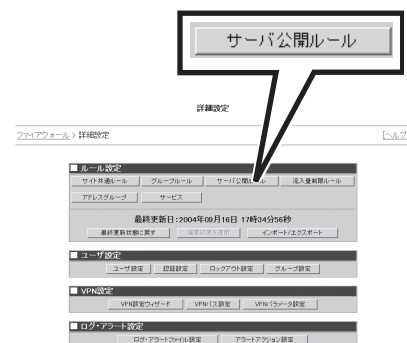
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

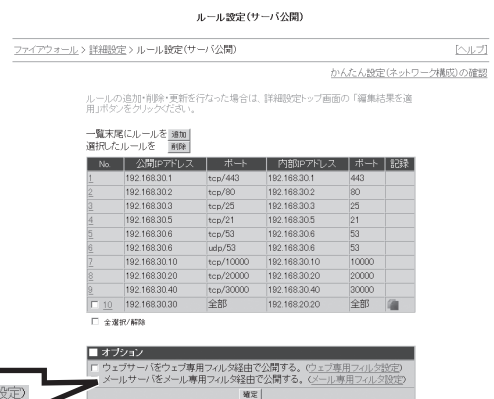
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。

詳細設定メニュー画面

4. 「オプション」の[メール専用フィルタ設定]をクリックする。

   メール専用フィルタ設定（外→内）画面が表示されます。

No.	公開IPアドレス	ポート	内部IPアドレス	ポート	記録
1	192.168.30.1	tcp/443	192.168.30.1	443	
2	192.168.30.2	tcp/80	192.168.30.2	80	
3	192.168.30.3	tcp/25	192.168.30.3	25	
4	192.168.30.5	tcp/21	192.168.30.5	21	
5	192.168.30.6	tcp/53	192.168.30.6	53	
6	192.168.30.6	udp/53	192.168.30.6	53	
7	192.168.30.10	tcp/10000	192.168.30.10	10000	
8	192.168.30.20	tcp/20000	192.168.30.20	20000	
9	192.168.30.40	tcp/30000	192.168.30.40	30000	
□ 10	192.168.30.30	全部	192.168.20.20	全部	

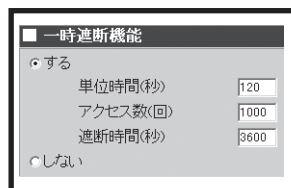
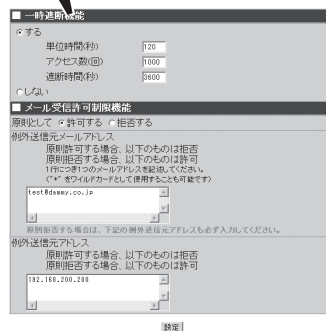
サーバ公開ルール一覧画面

5. 一時遮断機能の利用の有無を選択する。利用する場合は、単位時間、アクセス数、遮断時間を設定する。

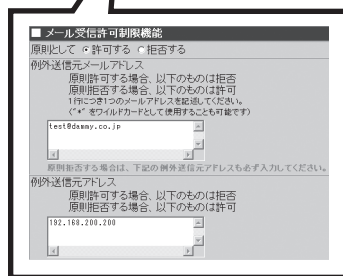
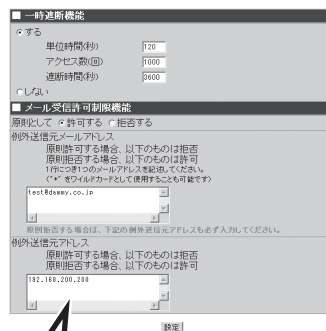
メール専用フィルタ設定(外→内)画面

ヒント

一時遮断機能によって、外部ネットワークの特定の端末から内部ネットワーク上のメールサーバに過剰アクセスする攻撃(DoS攻撃)を回避します。指定する単位時間あたり、指定するアクセス数を越えて接続した場合、その送信元からのメールアクセスを指定した遮断時間の間制限します。

さらに、一時遮断機能を有効にしていると、外部ネットワークの過剰な数の端末から内部ネットワーク上のメールサーバにアクセスする攻撃(DDoS攻撃)についても回避します。この場合は指定する単位時間あたり、50を超える送信元からのメールアクセスを制限します。

6. メール受信許可制限機能を設定する。

メール専用フィルタ設定(外→内)画面

- 原則として許可する
  メールサーバに対するアクセスを原則として許可する場合に選択します。
  例外として拒否するメールアドレスがある場合には、例外送信元メールアドレスのテキストエリアに拒否対象となるメールアドレスを指定します。例外として拒否するネットワーク、端末がある場合には、例外送信元アドレスのテキストエリアに、拒否対象となるネットワークアドレスまたはIPアドレスを設定します。
- 原則として拒否する
  メールサーバに対するアクセスを原則として拒否する場合に選択します。
  例外として許可するメールアドレス、ネットワーク、端末がある場合には、例外送信元メールアドレスと例外送信元アドレスの両方を設定します。例外送信元メールアドレスのテキストエリアに、許可対象となるメールアドレスを設定します。例外送信元アドレスのテキストエリアに、許可対象となるネットワークアドレスまたはIPアドレスを設定します。
  なお、メールアドレス部分には、必ず有効なメールアドレスを指定してください。メールの送信時にはアドレスのチェックは行わないため、不正なアドレスが指定された場合、メールはそのまま送信され、エラーになる場合があります。

「原則として拒否する」を選択した場合、例外送信元メールアドレスと例外送信元アドレスの両方の条件に合うメールだけ許可します。したがって、両方の欄に値を指定してください。もし、送信元メールアドレスだけで許可を決定したい場合、例外送信元アドレスの方には、0.0.0.0/0のようにネットマスク部分を0(=全ネットワーク)と指定します。

7. [設定]をクリックする。

   メール専用フィルタ設定(外→内)結果画面が表示されます。

8. [ルール設定(サーバ公開)に戻る]をクリックする。

   サーバ公開ルール一覧画面が表示されます。

メール専用フィルタ設定(外→内)結果
ファイアウォール > 詳細設定 > ルール設定(サーバ公開) > メール専用フィルタ設定 > 設定結果 [ヘルプ]
設定しました。
詳細設定画面の「編集結果を適用」ボタンでルールが有効になります。
ルール設定(サーバ公開)に戻る
ルール設定(サーバ公開)に戻る

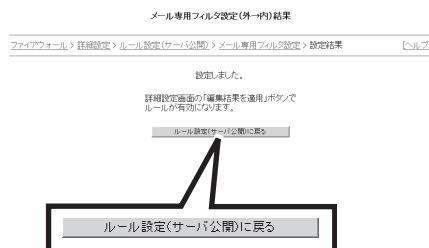
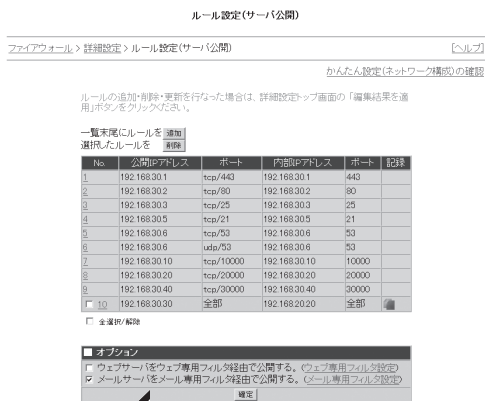
メール専用フィルタ設定(外→内)結果画面

9. 「メールサーバをメール専用フィルタ経由で公開する。」のチェックボックスにチェックし、[確定]をクリックする。

   設定更新結果画面が表示されるので、[ルール設定(サーバ公開)に戻る]をクリックします。

重要

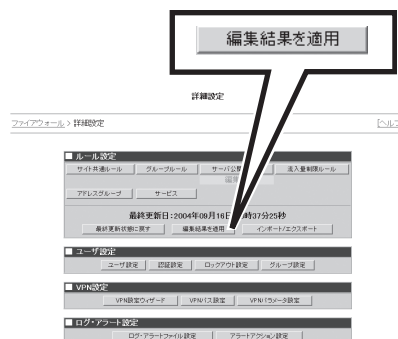
確定をクリックしないと、メール専用フィルタ設定をしてもフィルタリング機能は有効になりません。逆にメール専用フィルタ設定をしないでフィルタリング機能を有効にしても効果はありません。

No.	公開IPアドレス	ポート	内部IPアドレス	ポート	記録
1	192.168.30.1	tcp/443	192.168.30.1	443	
2	192.168.30.2	tcp/80	192.168.30.2	80	
3	192.168.30.3	tcp/25	192.168.30.3	25	
4	192.168.30.5	tcp/21	192.168.30.5	21	
5	192.168.30.6	tcp/53	192.168.30.6	53	
6	192.168.30.6	udp/53	192.168.30.6	53	
7	192.168.30.10	tcp/10000	192.168.30.10	10000	
8	192.168.30.20	tcp/20000	192.168.30.20	20000	
9	192.168.30.40	tcp/30000	192.168.30.40	30000	
10	192.168.30.30	全部	192.168.20.20	全部	

サーバ公開ルール一覧画面

10. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

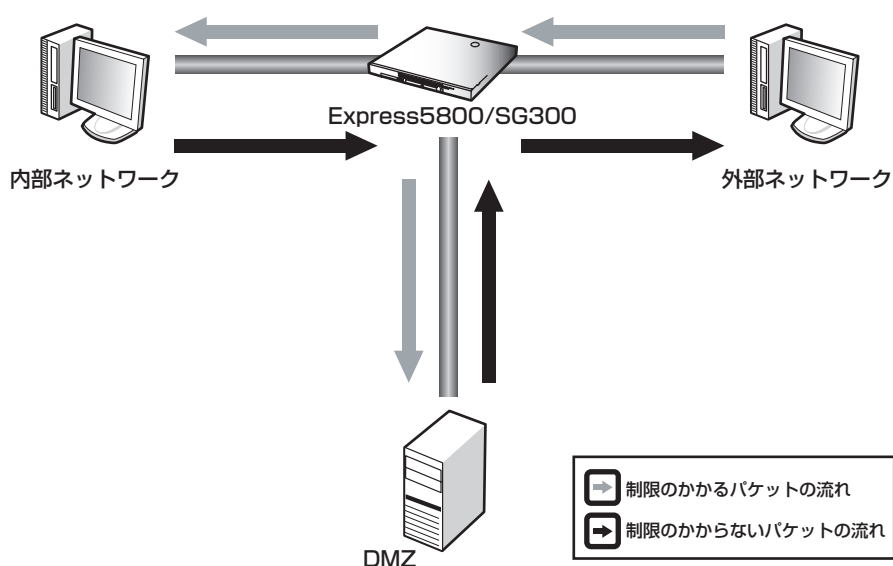
重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順9で[確定]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はフィルタリング機能の設定前の状態に戻ります。**

11. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

    フィルタリング設定がExpress5800/SG300に適用され、設定結果画面が表示されます。

12. [詳細設定メニューに戻る]をクリックする。

流入量制限ルール

流入量制限ルールとは、各インタフェースを介して内部方向に流入するパケットを監視し、流入量が設定した値を超えた場合は、Express5800/SG300を越えての新規の接続要求を拒否する機能のことです。
パケット量は、宛先や送信元、ポートによらず、指定したインタフェースに流れる全パケットの総量を測ります。
なお、流入量制限は通信の片方向だけに掛かります。外部ネットワークからExpress5800/SG300へ流入する方向と、Express5800/SG300を経て内部ネットワーク/DMZへ流入する方向に制限をかける場合でも、内部ネットワーク/DMZから外部ネットワークへの通信は影響を受けません。
これにより、DoS攻撃などの過負荷となる通信から内部サーバを保護することができます。

流入量ルール制限

流入量制限ルールでは以下の項目を設定します。

- 流入量制限ルールの設定内容の確認
- 流入量制限ルールの追加
- 流入量制限ルールの削除
- 流入量制限ルールの更新

流入量制限ルールの設定内容の確認

Express5800/SG300は設定されたインタフェースの流入量を監視し、流入量の上限を超えると、ファイアウォールを越えての新規の接続要求を拒絶するようになります。

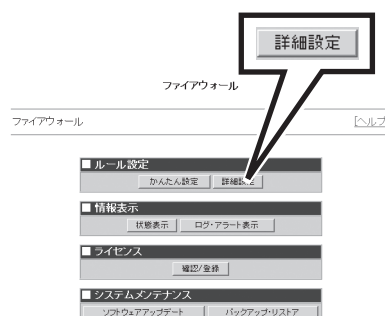
かんたん設定で不正アクセス対策レベルを「アドバンス」に設定した場合、外部からファイアウォールへのパケット流入量を70Mbpsに制限します。

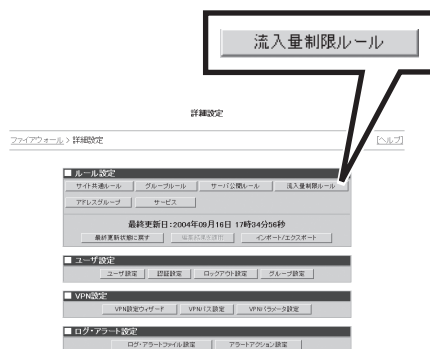
流入方向や制限値は、流入量制限ルールで変更することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[流入量制限ルール]をクリックする。

詳細設定メニュー画面

流入量制限ルール一覧画面が表示されます。表示される内容は以下の通りです。

項　目	説　明
No.	ルールの番号です。
流入方向	制限を掛ける流入方向を表示します。
制限値	指定する方向に流入するパケット量の上限値です。

ルール設定(流入量制限)

ファイアウォール > 詳細設定 > ルール設定(流入量制限) [ヘルプ]

かんたん設定(ネットワーク構成)の確認

ルールの追加・削除・更新を行なった場合は、詳細設定トップ画面の「編集結果を適用」ボタンをクリックください。

一覧末尾にルールを 追加
選択したルールを 削除

No.	流入方向	制限値
□ 1	ファイアウォール→DMZ(172.16.16.0/25)	10 Mbps
□ 2	外部→ファイアウォール	10 Mbps

□ 全選択/解除

流入量制限ルール一覧画面

画面右上の「かんたん設定(ネットワーク構成)の確認」をクリックすると、かんたん設定で設定した内容が別ウィンドウで表示されます。

具体的な流入量制限ルール一覧の事例を示します。

No.	流入方向	制限値
□ 1	ファイアウォール→DMZ(172.16.16.0/25)	10 Mbps
□ 2	外部→ファイアウォール	10 Mbps

流入量制限ルール一覧画面

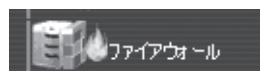
ルールの1行目: ファイアウォールからDMZへ流れるパケットの総流入量を10Mbpsに制限することを表します。

ルールの2行目: 外部ネットワークからファイアウォールへ流れるパケットの総流入量を10Mbpsに制限することを表します。

流入量制限ルールの追加

必要に応じて流入量制限ルールを追加することができます。

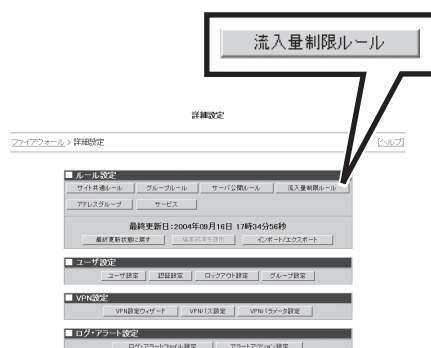
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

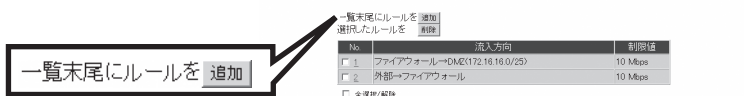
   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[流入量制限ルール]をクリックする。

   流入量制限ルール一覧画面が表示されます。

詳細設定メニュー画面

4. 「一覧末尾にルールを『追加』」をクリックする。

   ルール設定追加画面が表示されます。

流入量制限ルール一覧画面

5. ルール設定追加画面に表示される各項目を設定する。

- 流入方向
  流入方向をラジオボタンで選択します。
- 制限
  指定した方向に流入するパケット量の上限値を設定します。Mbps単位による指定ができます。入力できる範囲は1から1000までです。

ルール設定追加画面

6. [登録]をクリックする。

   追加結果画面が表示されます。

登録に失敗した場合には、エラー内容を示す画面を表示します。

7. [ルール設定(流入量制限)に戻る]をクリックする。

   追加したルールが反映された流入量制限ルール画面が表示されます。

追加結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの追加前の状態に戻ります。**

詳細設定メニュー画面

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しく追加したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。

流入量制限ルールの削除

不要になった流入量制限ルールを削除することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

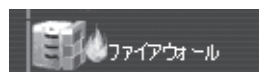
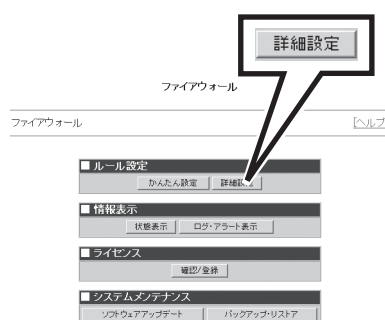
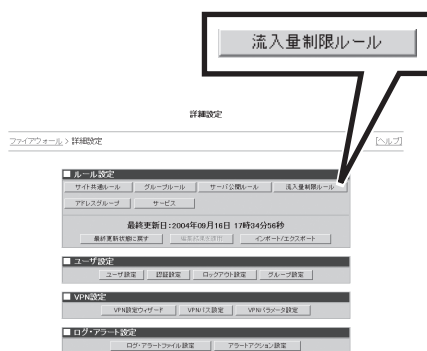
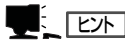
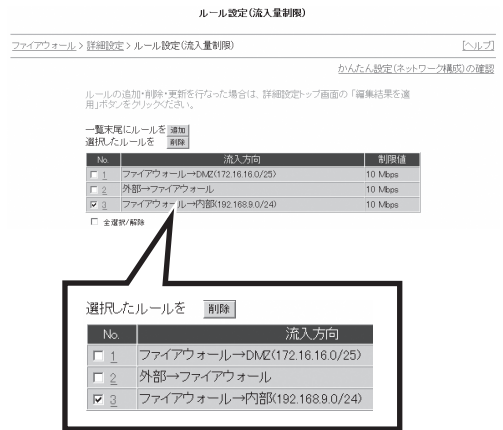
ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[流入量制限ルール]をクリックする。

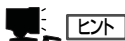
   流入量制限ルール一覧画面が表示されます。

詳細設定メニュー画面

4. 削除したいルールの「No.」の横に表示されるチェックボックスをチェックし、「選択したルールを『削除』」をクリックする。

ヒント

「全選択/解除」のチェックボックスをチェックすると、削除可能なルールのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのルールを削除対象から外すこともできます。

流入量制限ルール一覧画面

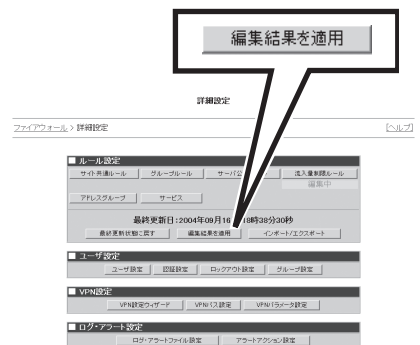
5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

ヒント

[キャンセル]をクリックすると、削除されずに流入量制限ルール一覧画面に戻ります。

流入量制限ルールが削除され、削除を反映した流入量制限ルール一覧画面が表示されます。

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順5で[OK]をクリックしますが、この段階ではルールの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの削除前の状態に戻ります。**

詳細設定メニュー画面

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

ルールの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。

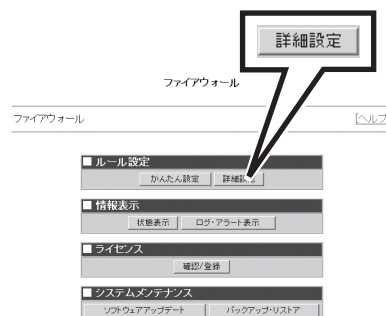
流入量制限ルールの更新

一度設定した流入量制限ルールの制限値を変更することができます。

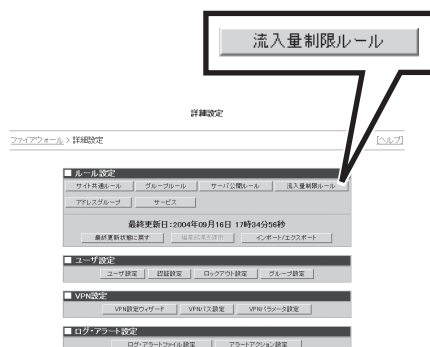
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

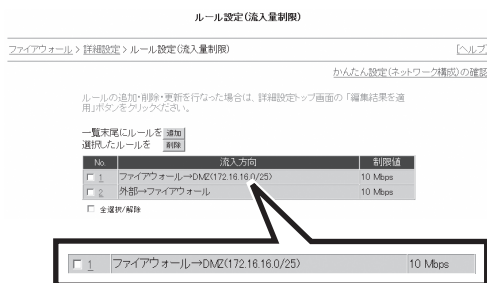
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

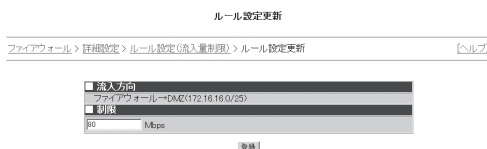
   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[流入量制限ルール]をクリックする。

   流入量制限ルール一覧画面が表示されます。

詳細設定メニュー画面

4. 変更したいルールの「No.」をクリックする。

   ルール設定更新画面が表示されます。

流入量制限ルール一覧画面

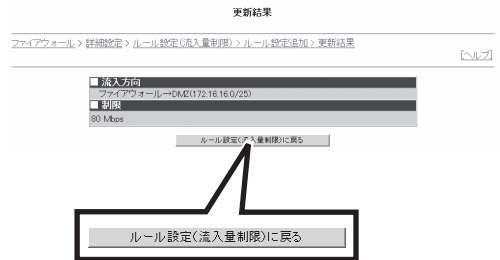
5. ルール設定更新画面からパケット流入量の制限値を設定する。

ルール設定更新画面

6. [登録]をクリックする。

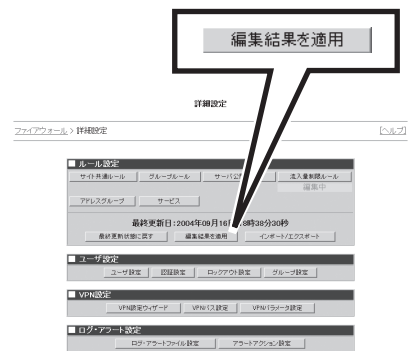
更新結果画面が表示されます。

> ✔ チェック
>
> 登録に失敗した場合には、エラー内容を示す画面を表示します。

7. [ルール設定(流入量制限)に戻る]をクリックする。

更新したルールが反映された流入量制限ルール一覧画面が表示されます。

更新結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

> **重要**
>
> - **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
> - **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの更新前の状態に戻ります。**

詳細設定メニュー画面

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

更新したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。

アドレスグループ

アドレスグループとは、1つ以上のホストアドレスまたはネットワークアドレスをグループ化したもので、ユーザが自由に設定することができます。設定したアドレスグループはサイト共通ルール、グループルールのルール設定の際に送信元、宛先として指定することができます。これにより、簡単に環境に合わせたフィルタリング設定ができます。
アドレスグループは、ホスト、ネットワーク、ホストおよびネットワークを複数含むグループの3つに分けて考えることができます。
アドレスグループでは、以下のような設定・管理を行うことができます。

- アドレスグループの確認
- アドレスグループの追加
- アドレスグループの削除
- アドレスグループの更新

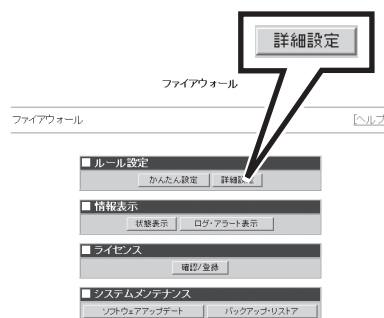
アドレスグループの確認

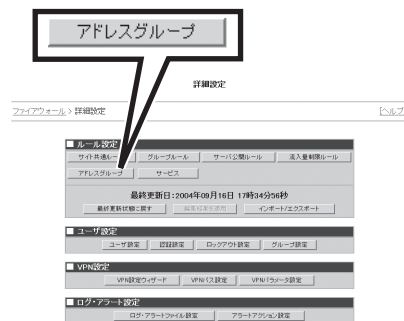
すでに設定したアドレスグループはアドレスグループ一覧画面から確認することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[アドレスグループ]をクリックする。

詳細設定メニュー画面

アドレスグループ一覧画面が表示されます。表示される内容は以下の通りです。

項　目	説　明	
名前	アドレスグループの種別を示すアイコンとアドレスグループの名称です。	
		（ホスト） 単一のホストアドレスを登録したときにこのアイコンを設定します。
		（ネットワーク） ネットワークアドレスを登録したときにこのアイコンを設定します。
		（グループ） ホストアドレス、ネットワークアドレスを複数登録したときにこのアイコンを設定します。
メンバ	設定したアドレスグループに所属するホストアドレス、ネットワークアドレスを表示します。	

ルール設定(アドレスグループ)

ファイアウォール > 詳細設定 > ルール設定(アドレスグループ)　[ヘルプ]

アドレスグループを　追加
選択したアドレスグループを　削除

名前	メンバ
部門ネット1	192.168.20.0/24
部門ネット2	192.168.30.0/24
ウェブサーバ	192.168.10.101
メールサーバ	192.168.10.102
公開サーバ	192.168.10.101, 192.168.10.102
東京営業所	192.168.128.0/17, 192.168.100.0/24
DBサーバ	192.168.20.105

□全選択／解除

アドレスグループ一覧画面

具体的なアドレスグループ一覧の事例を示します。

- 上記画面の部門ネット1

  ネットワークアドレス192.168.20.0/24のネットワークが登録されたアドレスグループです。

- 上記画面のウェブサーバ

  IPアドレス192.168.10.101のホストが登録されたアドレスグループです。

- 上記画面の東京営業所

  ネットワークアドレス192.168.128.0/17、192.168.100.0/24が登録されたアドレスグループです。

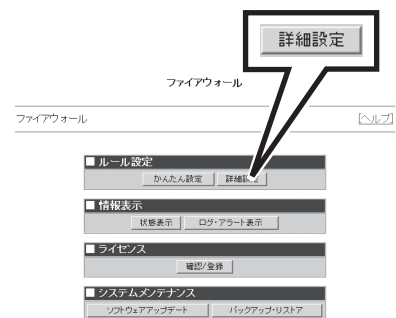
アドレスグループの追加

必要に応じてアドレスグループを追加することができます。

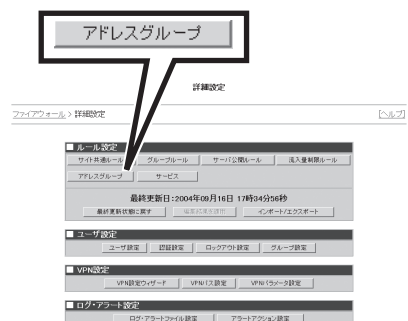
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

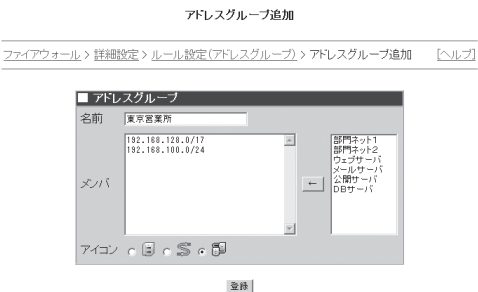
3. 詳細設定メニューの「ルール設定」から[アドレスグループ]をクリックする。

   アドレスグループ一覧画面が表示されます。

詳細設定メニュー画面

4. 「アドレスグループを『追加』」をクリックする。

   アドレスグループ追加画面が表示されます。

アドレスグループ一覧画面

5. アドレスグループ追加画面に表示される各項目を設定する。

アドレスグループ追加画面

項　目	説　明	
名前	アドレスグループの名称です。 最大で32バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)が使用できます。全角文字（日本語）も使用できます。既存のアドレスグループと重複する名前は付けられません。	
メンバ	設定するアドレスグループに所属するホストアドレス、ネットワークアドレスを登録します。 1行に1アドレスを入力します。 右側に既存のアドレスグループが表示されますので、アドレスグループを選択し、[←]をクリックすることでそのメンバを取り込むこともできます。	
アイコン		（ホスト） 単一のホストアドレスを登録したときにこのアイコンを設定します。
		（ネットワーク） ネットワークアドレスを登録したときにこのアイコンを設定します。
		（グループ） ホストアドレス、ネットワークアドレスを複数登録したときにこのアイコンを設定します。

ヒント

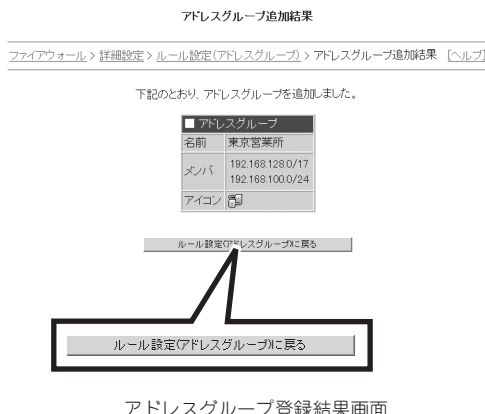
- 同じアドレスを複数登録した場合は、2つ目以降が自動的に削除されて登録されます。
- アドレスグループが含むことのできるメンバの数は、最大50個までです。

6. [登録]をクリックする。

アドレスグループ登録結果画面が表示されます。

登録に失敗した場合には、エラー内容を示す画面を表示します。

7. ［ルール設定（アドレスグループ）に戻る］をクリックする。

追加したアドレスグループが反映されたアドレスグループ一覧画面が表示されます。

アドレスグループ追加結果

ファイアウォール > 詳細設定 > ルール設定(アドレスグループ) > アドレスグループ追加結果 [ヘルプ]

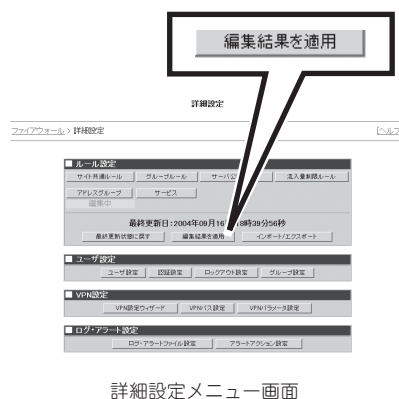
下記のとおり、アドレスグループを追加しました。

アドレスグループ登録結果画面

8. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はアドレスグループの追加前の状態に戻ります。**

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

新しく追加したアドレスグループがExpress5800/SG300に適用され、設定結果画面が表示されます。

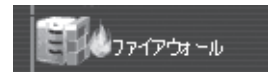
10. ［詳細設定メニューに戻る］をクリックする。

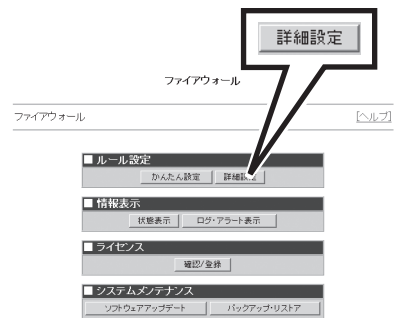
詳細設定

アドレスグループの削除

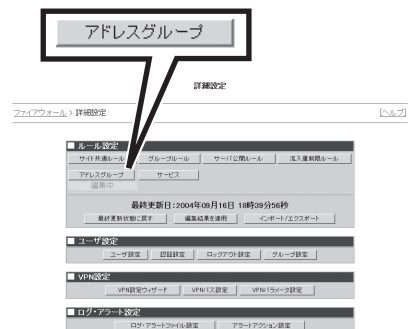
不要になったアドレスグループを削除することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[アドレスグループ]をクリックする。

   アドレスグループ一覧画面が表示されます。

詳細設定メニュー画面

4. 削除したいアドレスグループの「名前」の横に表示されるチェックボックスをチェックし、「選択したアドレスグループを『削除』」をクリックする。

   ヒント

   「全選択/解除」のチェックボックスをチェックすると、削除可能なアドレスグループのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのアドレスグループを削除対象から外すこともできます。

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

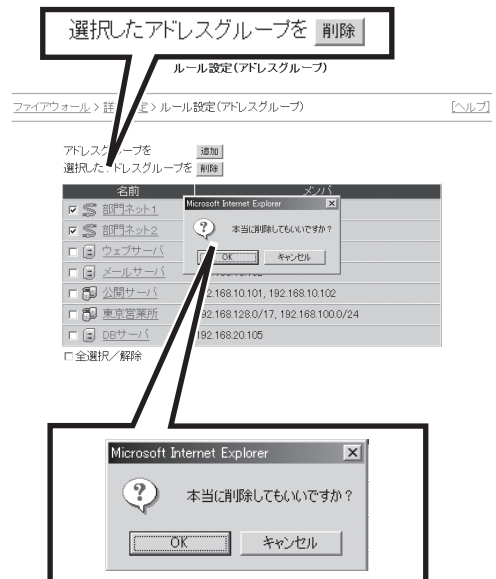
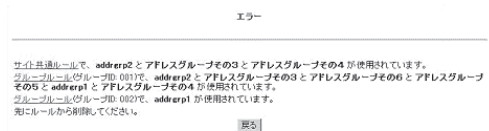
   ヒント

   [キャンセル]をクリックすると、削除されずにアドレスグループ一覧画面に戻ります。

   アドレスグループが削除され、削除を反映したアドレスグループ一覧画面が表示されます。

   チェック

   選択したアドレスグループが、サイト共通ルールまたはグループルールで指定されている場合、削除することができません。その場合、エラー内容を示す画面が表示されます。

   エラーの説明文中に表示される、サイト共通ルール、グループルールのリンクをクリックすると、それぞれサイト共通ルール一覧画面、グループルール一覧画面が表示されます。先にルールからアドレスグループを削除し、再度アドレスグループの削除を行ってください。

アドレスグループ一覧画面

エラー

サイト共通ルールで、addrgrp2 と アドレスグループその3 と アドレスグループその4 が使用されています。
グループルール(グループID: 001)で、addrgrp2 と アドレスグループその3 と アドレスグループその6 と アドレスグループその5 と addrgrp1 と アドレスグループその4 が使用されています。
グループルール(グループID: 002)で、addrgrp1 が使用されています。
先にルールから削除してください。

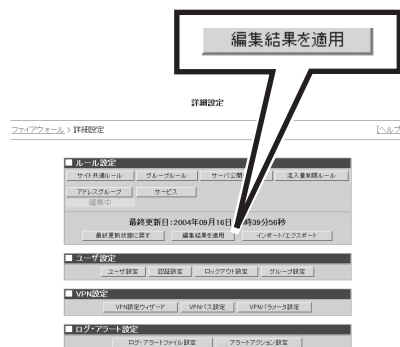
戻る

エラー内容を示す画面

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順5で[OK]をクリックしますが、この段階ではアドレスグループの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はアドレスグループの削除前の状態に戻ります。

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   アドレスグループの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。

ファイアウォール機能の設定方法

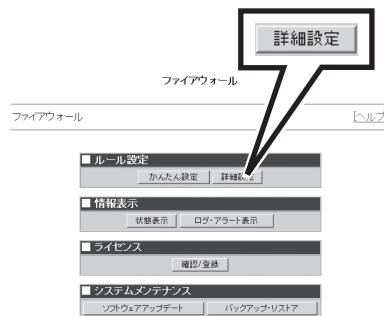
アドレスグループの更新

一度設定したアドレスグループの内容を変更することができます。

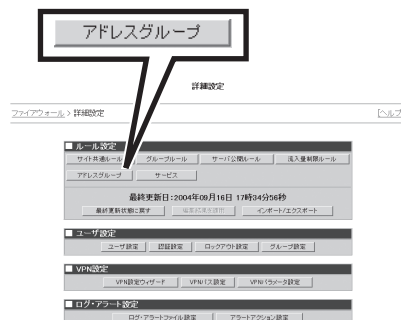
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[アドレスグループ]をクリックする。

   アドレスグループ一覧画面が表示されます。

詳細設定メニュー画面

4. 変更したいアドレスグループの「名前」をクリックする。

アドレスグループ更新画面が表示されます。

ルール設定(アドレスグループ)

ファイアウォール > 詳細設定 > ルール設定(アドレスグループ) [ヘルプ]

アドレスグループを 追加
選択したアドレスグループを 削除

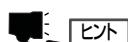
名前	メンバ
部門ネット1	192.168.20.0/24
部門ネット2	192.168.30.0/24
ウェブサーバ	192.168.10.101
メールサーバ	192.168.10.102
公開サーバ	192.168.10.101, 192.168.10.102
東京営業所	192.168.128.0/17, 192.168.100.0/24
DBサーバ	192.168.20.105

□全選択/解除

東京営業所 192.168.128.0/17, 192.168.100.0/24

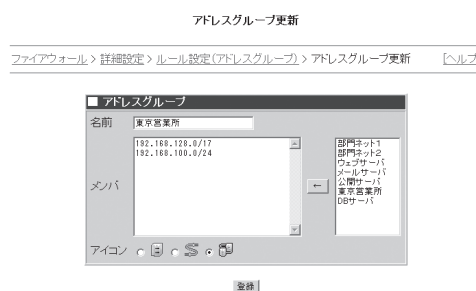
アドレスグループ一覧画面

5. アドレスグループ更新画面に表示される各項目を設定する。

ヒント

- 同じアドレスを複数登録した場合は、2つ目以降が自動的に削除されて登録されます。
- アドレスグループが含むことのできるメンバの数は、最大50個までです。

アドレスグループ更新

ファイアウォール > 詳細設定 > ルール設定(アドレスグループ) > アドレスグループ更新 [ヘルプ]

登録

アドレスグループ更新画面

項　目	説　明	
名前	アドレスグループの名称です。 最大で32バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)が使用できます。全角文字(日本語)も使用できます。既存のアドレスグループと重複する名前は付けられません。	
メンバ	設定するアドレスグループに所属するホストアドレス、ネットワークアドレスを登録します。 1行に1アドレスを入力します。 右側に既存のアドレスグループが表示されますので、アドレスグループを選択し、[←]をクリックすることでそのメンバを取り込むこともできます。	
アイコン		(ホスト) 単一のホストアドレスを登録したときにこのアイコンを設定します。
		(ネットワーク) ネットワークアドレスを登録したときにこのアイコンを設定します。
		(グループ) ホストアドレス、ネットワークアドレスを複数登録したときにこのアイコンを設定します。

6. [登録]をクリックする。

アドレスグループ更新結果画面が表示されます。

7. ［ルール設定（アドレスグループ）に戻る］をクリックする。

   更新したアドレスグループが反映されたアドレスグループ一覧画面が表示されます。

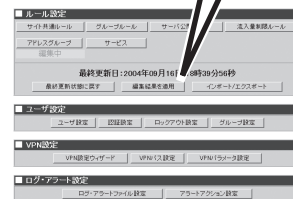
アドレスグループ更新結果

ファイアウォール > 詳細設定 > ルール設定（アドレスグループ） > アドレスグループ更新結果 ［ヘルプ］

下記のとおり、アドレスグループを更新しました。

ルール設定（アドレスグループ）に戻る

アドレスグループ更新結果画面

8. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。

   重要

   - **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
   - **[最終更新状態に戻す]をクリックすると、Express5800/SG300はアドレスグループの更新前の状態に戻ります。**

詳細設定メニュー画面

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

   更新したアドレスグループがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. ［詳細設定メニューに戻る］をクリックする。

サービス

サービスとは、通信種別(プロトコル)ごとのタイプ指定(ポート番号、ICMPタイプなど)をグループ化したもので、ユーザが自由に設定することができます。設定したサービスはサイト共通ルール、グループルールの通信種別として指定することができます。これにより、簡単に環境に合わせたフィルタリング設定ができます。
サービスでは、以下のような設定管理を行うことができます。

- サービスの確認
- サービスの追加
- サービスの削除
- サービスの更新

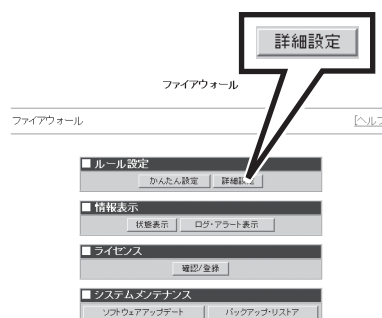
サービスの確認

すでに設定したサービスや標準定義サービスはサービス一覧画面から確認することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

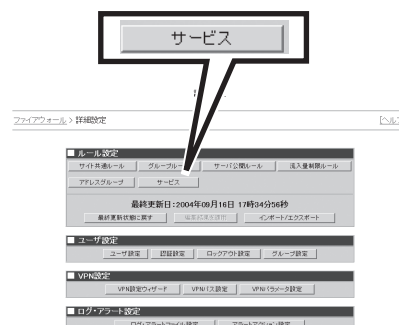
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サービス]をクリックする。

   サービス一覧画面が表示されます。表示される内容は以下の通りです。

項　目	説　明
名前	サービスの名前です。
メンバ	サービスの種別を表示します。

詳細設定メニュー画面

ヒント

「標準定義サービス」をクリックすると、あらかじめシステムで定義されたサービスの一覧を表示します。標準定義サービスはピンク色で表示され、変更・削除することができません。

「全サービス一覧」をクリックすると、ユーザ定義サービスと標準定義サービスを一覧表示します。

「ユーザ定義サービス」をクリックするとユーザ定義サービスの一覧を表示します。詳細設定メニューから画面を表示した場合は、ユーザ定義サービスの一覧が表示されています。

ルール設定（サービス）

ファイアウォール > 詳細設定 > ルール設定（サービス） [ヘルプ]

サービスを 追加
選択したサービスを 削除

ユーザ定義サービス一覧 標準定義サービス一覧 全サービス一覧

名前	メンバ
□ ウェブサービス	tcp/80, tcp/443
□ ファイル転送	tcp/21
□ アプリケーションA	tcp/50080
□ 共通サービス	tcp/25, tcp/80, tcp/443, tcp/110, tcp/53, udp/53, tcp/389

□全選択／解除

サービス一覧画面

具体的なサービス一覧の事例を示します。

上記画面のウェブサービス
TCPポート80のサービス（HTTP通信）、443のサービス（HTTPS通信）を含むサービスとして定義されています。

上記画面のファイル転送
TCPポート21のサービス（FTP通信）として定義されています。

上記画面のアプリケーションA
TCPポート50080のサービスとして定義されています。

上記画面の共通サービス
TCPポート25のサービス（SMTP通信）、80のサービス（HTTP通信）、443のサービス（HTTPS通信）、110のサービス（POP通信）、53のサービス（DNS通信）、389のサービス（LDAP通信）、UDPポート53のサービス（DNS通信）を含むサービスとして定義されています。

サービスの追加

必要に応じてサービスを追加することができます。

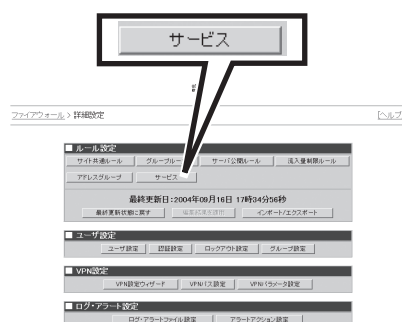
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

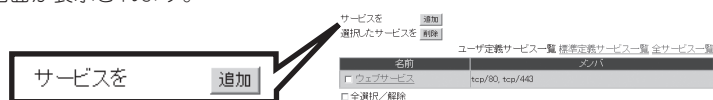
   詳細設定メニュー画面が表示されます。

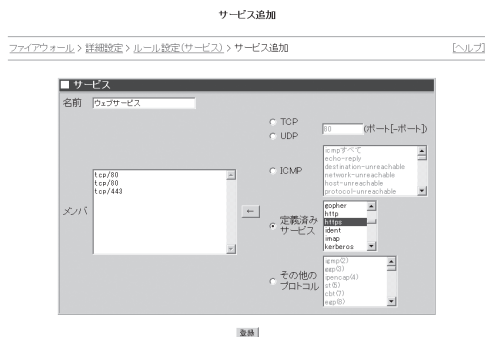
ファイアウォールメニュー画面

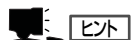
3. 詳細設定メニューの「ルール設定」から[サービス]をクリックする。

   サービス一覧画面が表示されます。

詳細設定メニュー画面

4. 「サービスを『追加』」をクリックする。

   サービス追加画面が表示されます。

サービス一覧画面

5. サービス追加画面に表示される各項目を設定する。

サービス追加画面

項　目	説　明	
名前	サービスの名称です。 最大で32バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)が使用できます。全角文字（日本語）も使用できます。既存のサービスと重複する名前は付けられません。	
メンバ	TCP/UDP	ラジオボタンを選択し、ポート番号を指定します。ハイフン(-)で区切って範囲を指定することができます。指定後、[←]をクリックすることで登録します。
	ICMP	ラジオボタンを選択し、右側のリストボックスからタイプを指定して[←]をクリックすることで登録します。
	定義済みサービス	ラジオボタンを選択し、右側のリストボックスから選択して[←]をクリックすることで登録します。
	その他のプロトコル	ラジオボタンを選択し、右側のリストボックスから選択して[←]をクリックすることで登録します。

- 同じメンバを複数登録した場合は、2つ目以降が自動的に削除されて登録されます。
- サービスが含むことのできるメンバの数は、最大50個までです。

6. [登録]をクリックする。

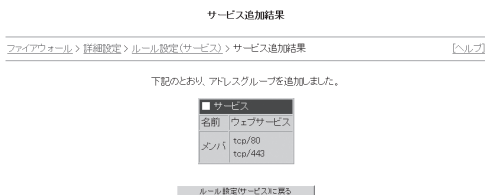
サービス追加結果画面が表示されます。

チェック

登録に失敗した場合には、エラー内容を示す画面を表示します。

7. [ルール設定(サービス)に戻る]をクリックする。

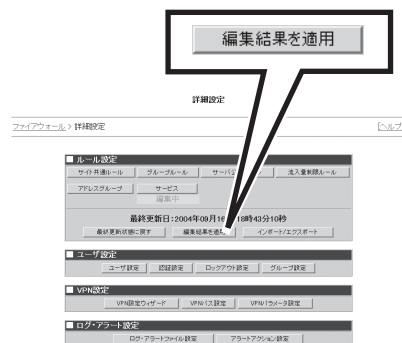
追加したサービスが反映されたサービス一覧画面が表示されます。

ルール設定(サービス)に戻る

サービス追加結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はサービスの追加前の状態に戻ります。**

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しく追加したサービスがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。

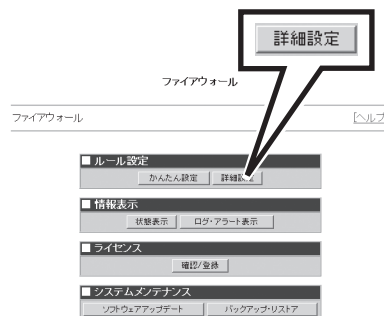
サービスの削除

不要になったユーザ定義サービスを削除することができます。
標準定義サービスは削除できません。

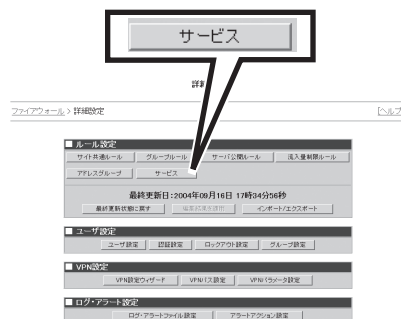
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

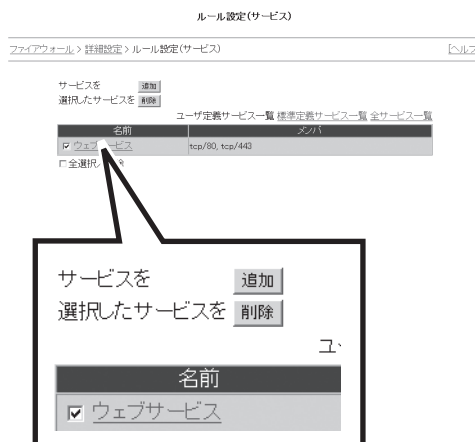
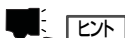
   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サービス]をクリックする。

   サービス一覧画面が表示されます。

詳細設定メニュー画面

4. 削除したいサービスの「名前」の横に表示されるチェックボックスをチェックし、「選択したサービスを『削除』」をクリックする。

   ヒント

   「全選択/解除」のチェックボックスをチェックすると、削除可能なサービスのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのサービスを削除対象から外すこともできます。

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

> ヒント
>
> [キャンセル]をクリックすると、削除されずにサービス一覧画面に戻ります。

サービスが削除され、削除を反映したサービス一覧画面が表示されます。

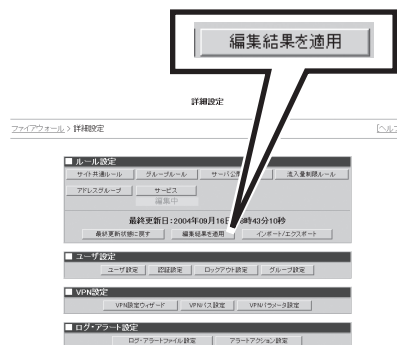
> チェック
>
> 選択したサービスが、サイト共通ルールまたはグループルールで指定されている場合、削除することができません。その場合、エラー内容を示す画面が表示されます。
>
> エラーの説明文中に表示される、サイト共通ルール、グループルールのリンクをクリックすると、それぞれサイト共通ルール一覧画面、グループルール一覧画面が表示されます。先にルールからサービスを削除し、再度サービスの削除を行ってください。

エラー

サイト共通ルールで、aaaa と サービス1 と bbbb が使用されています。
グループルール(グループID: 001)で、サービス1 と サービス2 が使用されています。
先にルールから削除してください。
戻る

エラー内容を示す画面

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

> 重要
>
> - 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。
>
>   手順5で[OK]をクリックしますが、この段階ではサービスの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
> - [最終更新状態に戻す]をクリックすると、Express5800/SG300はサービスの削除前の状態に戻ります。

詳細設定メニュー画面

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

サービスの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。

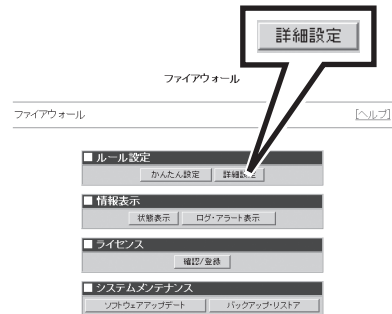
サービスの更新

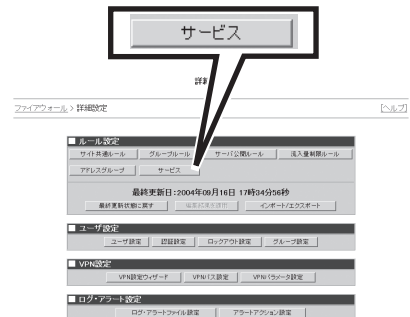
一度設定したサービスの内容を変更することができます。
標準定義サービスは変更できません。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

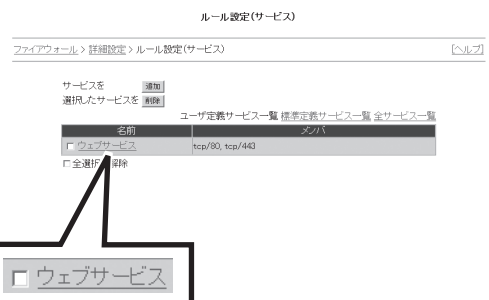
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サービス]をクリックする。

   サービス一覧画面が表示されます。

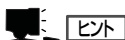
詳細設定メニュー画面

4. 変更したいサービスの「名前」をクリックする。

   サービス更新画面が表示されます。

サービス一覧画面

5. サービス更新画面に表示される各項目を設定する。

サービス更新画面

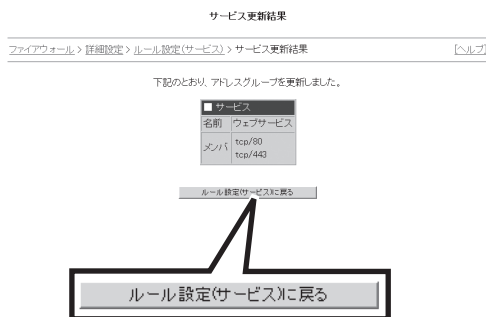
<table>
<tr><th>項　目</th><th colspan="2">説　明</th></tr>
<tr><td>名前</td><td colspan="2">サービスの名称です。
最大で32バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)が使用できます。全角文字（日本語）も使用できます。既存のサービスと重複する名前は付けられません。</td></tr>
<tr><td rowspan="4">メンバ</td><td>TCP/UDP</td><td>ラジオボタンを選択し、ポート番号を指定します。指定後、[←]をクリックすることで登録します。</td></tr>
<tr><td>ICMP</td><td>ラジオボタンを選択し、右側のリストボックスからタイプを指定して[←]をクリックすることで登録します。</td></tr>
<tr><td>定義済みサービス</td><td>ラジオボタンを選択し、右側のリストボックスから選択して[←]をクリックすることで登録します。</td></tr>
<tr><td>その他のプロトコル</td><td>ラジオボタンを選択し、右側のリストボックスから選択して[←]をクリックすることで登録します。</td></tr>
</table>

ヒント

- 同じメンバを複数登録した場合は、2つ目以降が自動的に削除されて登録されます。
- サービスが含むことのできるメンバの数は、最大50個まででです。

6. [登録]をクリックする。

サービス更新結果画面が表示されます。

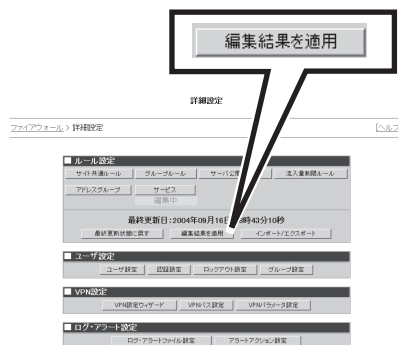
7. [ルール設定(サービス)に戻る]をクリックする。

更新したサービスが反映されたサービス一覧画面が表示されます。

サービス更新結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はサービスの更新前の状態に戻ります。**

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   更新したサービスがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。

ルール設定の履歴表示

「かんたん設定」や詳細設定メニューの「ルール設定」で設定できる各種ルールは、設定変更するたびに設定情報が履歴として保持されます。この履歴情報を利用することで、過去の設定内容を確認したり、日時を指定してその時点の設定内容に戻したりすることができます。

- 設定履歴を参照するには
- 過去の設定内容に戻すには
- 設定履歴を削除するには

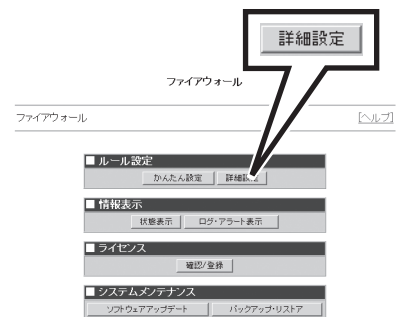
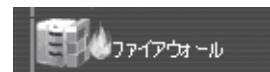
設定履歴を参照するには

日時を指定して設定した内容を参照することができます。

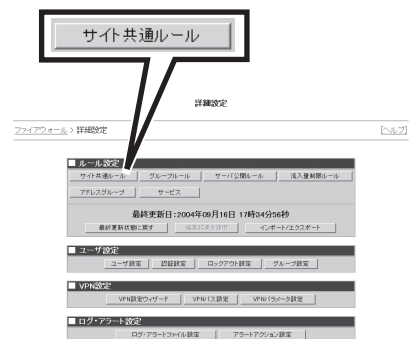
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

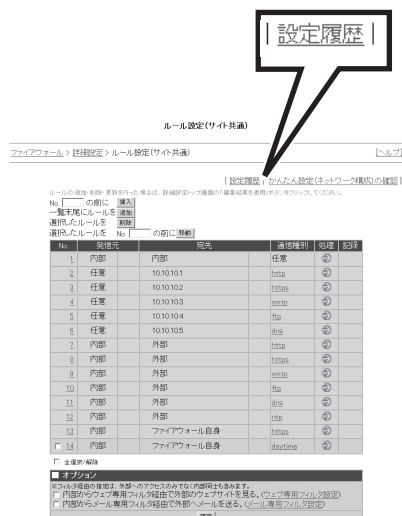
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

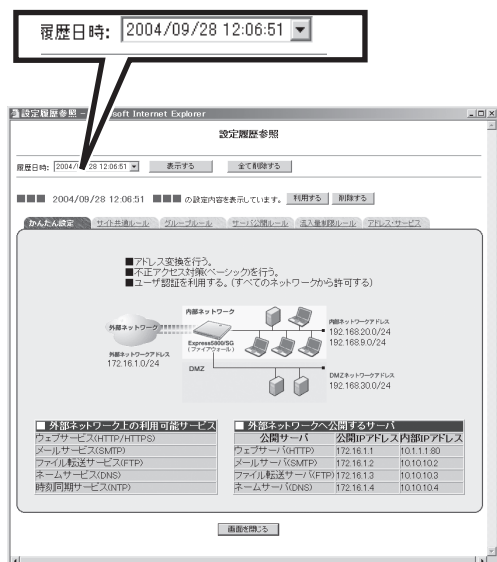
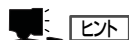
3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   サイト共通ルール設定一覧画面が表示されます。

詳細設定メニュー画面

4. 画面右上の「設定履歴」をクリックする。

   設定履歴参照画面が別ウィンドウで表示されます。

サイト共通ルール設定一覧画面

5. 「履歴日時」のプルダウンメニューを利用して表示したい日時を選択し、［表示する］をクリックする。

   指定した日時の履歴が表示されます。プルダウンメニューの下に現在表示している設定履歴の更新時間が表示されます。

設定履歴参照画面

ウィンドウを開いた直後は、その時点でもっとも新しい履歴が表示されます。

6. 「かんたん設定」、「サイト共通ルール」、「グループルール」、「サーバ公開ルール」、「流入量制限ルール」、「アドレス・サービス」のうち確認したい設定項目のタブをクリックする。

   それぞれの設定履歴が表示されます。

過去の設定内容に戻すには

指定した設定履歴の内容に設定を戻すことができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   サイト共通ルール設定一覧画面が表示されます。

詳細設定メニュー画面

4. 画面右上の「設定履歴」をクリックする。

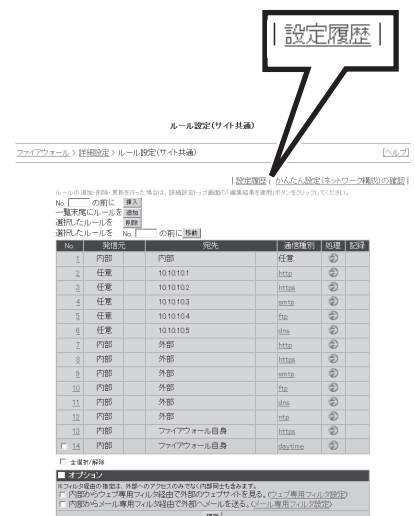
   設定履歴参照画面が別ウィンドウで表示されます。

サイト共通ルール設定一覧画面

5. 「履歴日時」のプルダウンメニューを利用して表示したい日時を選択し、[表示する]をクリックする。

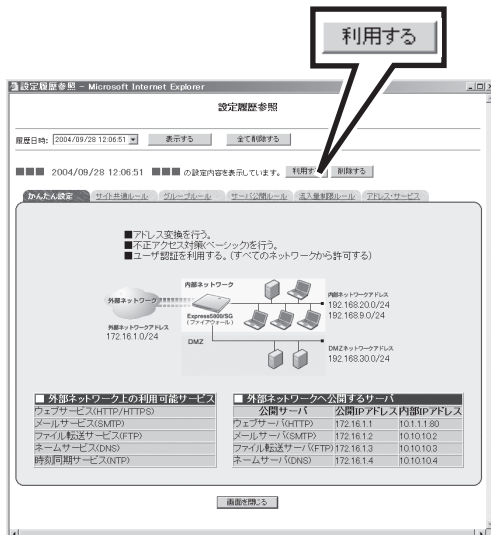
   指定した日時の履歴が表示されます。プルダウンメニューの下に現在表示している設定履歴の更新時間が表示されます。

設定履歴参照画面

ヒント

設定履歴参照画面を開いた直後は、その時点でもっとも新しい履歴が表示されます。

6. 「かんたん設定」、「サイト共通ルール」、「グループルール」、「サーバ公開ルール」、「流入量制限ルール」、「アドレス・サービス」のうち確認したい設定項目のタブをクリックする。

   それぞれの設定履歴が表示されます。

7. [利用する]をクリックする。

設定履歴参照画面

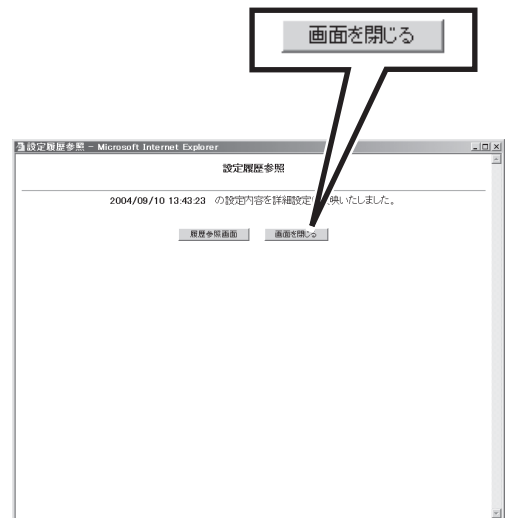
8. 別ウィンドウで利用確認ダイアログメッセージが表示されるので[OK]をクリックする。

重要

このとき、指定した日時のすべての設定履歴情報が反映されます。

チェック

このとき、詳細設定を編集中の場合は確認画面が表示されます。
[戻る]をクリックすると、設定履歴の反映を行わないで元の画面に戻ります。
[次へ]をクリックすると、設定中の詳細設定データを破棄して、設定履歴の反映に進みます。

9. 設定履歴参照画面は、反映結果が表示される。再度設定履歴を表示する場合は、[履歴参照画面]をクリック、設定履歴参照画面を閉じる場合は[画面を閉じる]をクリックする。

設定履歴参照画面

10. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

11. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

設定履歴がExpress5800/SG300に適用され、設定結果画面が表示されます。

12. [詳細設定メニューに戻る]をクリックする。

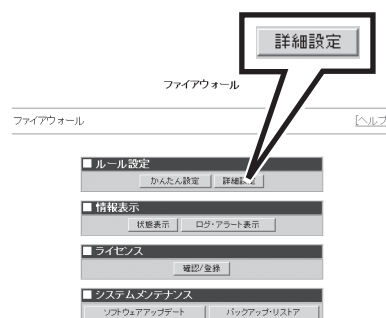
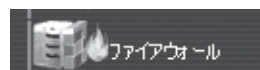
設定履歴を削除するには

設定履歴を削除することができます。

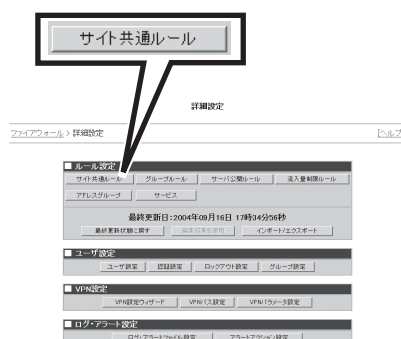
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   サイト共通ルール設定一覧画面が表示されます。

詳細設定メニュー画面

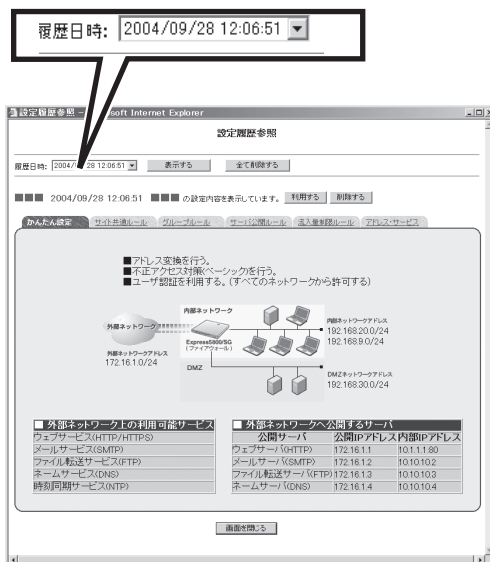
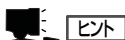
4. 画面右上の「設定履歴」をクリックすると、設定履歴参照画面が別ウィンドウで表示される。

サイト共通ルール設定一覧画面

5. 「履歴日時」のプルダウンメニューを利用して表示したい日時を選択し、[表示する]をクリックする。

   指定した日時の履歴が表示されます。プルダウンメニューの下に現在表示している設定履歴の更新時間が表示されます。

設定履歴参照画面

ヒント

設定履歴参照画面を開いた直後は、その時点でもっとも新しい履歴が表示されます。

6. 「かんたん設定」、「サイト共通ルール」、「グループルール」、「サーバ公開ルール」、「流入量制限ルール」、「アドレス・サービス」のうち確認したい設定項目のタブをクリックする。

   それぞれの設定履歴が表示されます。

7. [削除する]または[全て削除する]をクリックする。

   [削除する]をクリックした場合は、表示中の日時の設定履歴を削除します。
   [全てを削除する]をクリックした場合は、すべての設定履歴を削除します。

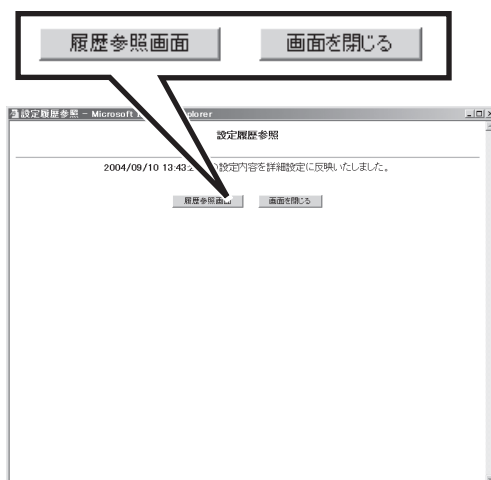
設定履歴参照画面

ファイアウォール機能の設定方法

8. 別ウィンドウで利用確認ダイアログメッセージが表示されるので[OK]をクリックする。

[削除する]をクリックした場合は、設定履歴参照画面に反映結果が表示される。

9. 再度設定履歴を表示する場合は[履歴参照画面]を、設定履歴参照画面を閉じる場合は[画面を閉じる]をクリックする。

[全てを削除する]をクリックした場合は、設定履歴参照画面に反映結果が表示さます。設定履歴参照画面を閉じる場合は[画面を閉じる]をクリックしてください。

設定履歴参照画面

インポート/エクスポート

詳細設定メニューの「ルール設定」で設定できる「サイト共通ルール」、「サーバ公開ルール」、「流入量制限ルール」、「サービス」、「アドレスグループ」の設定内容を記述したファイルをExpress5800/SG300からエクスポートしたり、インポートしたりすることができます。

- 設定内容のインポート
- 設定内容のエクスポート

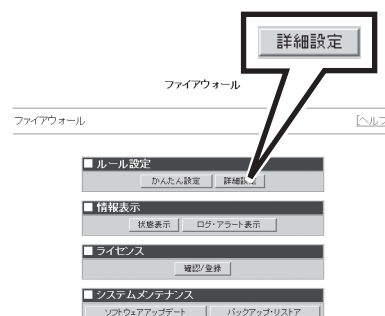
設定内容のインポート

詳細設定メニューの「ルール設定」で設定できる「サイト共通ルール」、「サーバ公開ルール」、「流入量制限ルール」、「サービス」、「アドレスグループ」の設定内容を記述したファイルをExpress5800/SG300にインポートすることができます。

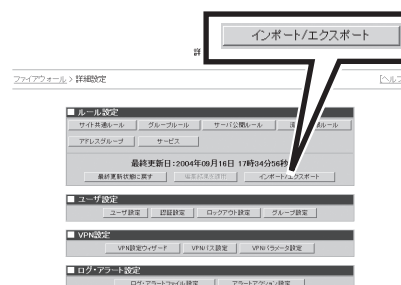
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

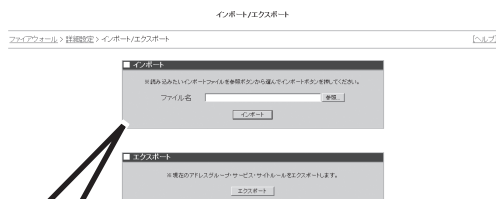
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[インポート/エクスポート]をクリックする。

   インポート/エクスポート画面が表示されます。

詳細設定メニュー画面

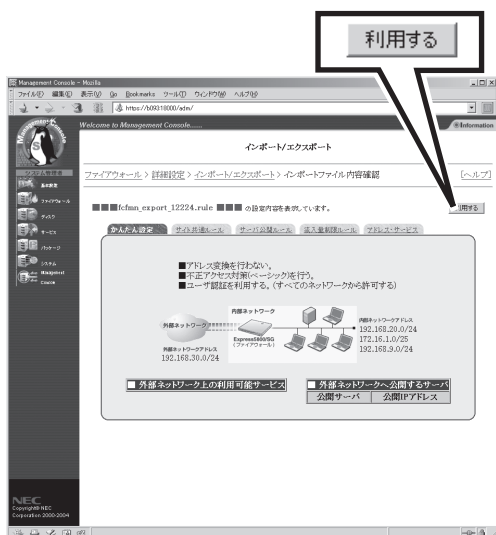
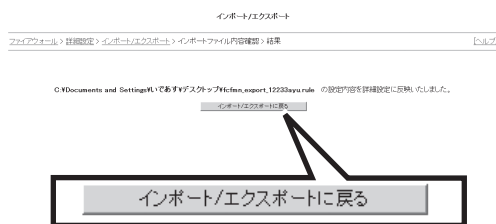
4. ［参照］をクリックしてインポートしたいファイルを指定し、［インポート］をクリックする。

インポートファイル内容確認画面が表示されます。各タブをクリックすると、設定内容が表示されます。

チェック

- ファイルのインタフェース情報が異なる場合は、インポートできません。エラーメッセージが表示され、［利用する］は使用できなくなります。
- ユーザが設定した「アドレスグループ」、「サービス」を利用してグループルールを設定している場合に、そのアドレスグループ、サービスが登録されていないファイルをインポートするとエラーになります。
- グループルールはインポート対象外です。

5. ［利用する］をクリックする。

6. 別ウィンドウで確認ダイアログメッセージが表示されるので［OK］をクリックする。

インポート結果確認画面が表示されます。

7. ［インポート/エクスポートに戻る］をクリックする。

インポート結果確認画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

インポートしたファイルの内容がExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。

ファイアウォール機能の設定方法

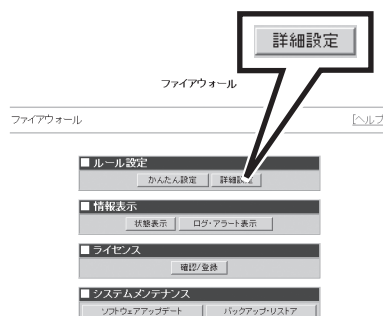
設定内容のエクスポート

詳細設定メニューの「ルール設定」で設定できる「サイト共通ルール」、「サーバ公開ルール」、「流入量制限ルール」、「サービス」、「アドレスグループ」の設定内容をファイルにエクスポートすることができます。

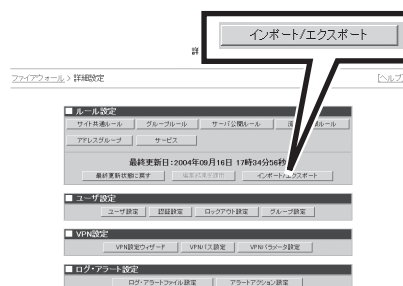
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[インポート/エクスポート]をクリックする。

   インポート/エクスポート画面が表示されます。

詳細設定メニュー画面

4. [エクスポート]をクリックする。

   ファイルのダウンロード画面が表示されます。保存をクリックして、保存先を指定します。

ユーザ設定

Express5800/SG300を利用してネットワークにアクセスするユーザの管理を行うことができます。
ユーザ設定では、以下の項目を設定/管理します。

ユーザ設定 .... Express5800/SG300が管理するユーザの登録、削除、変更が行えます。

認証設定 .... ユーザ認証を利用するかどうかを設定します。

ロックアウト設定 .... ユーザ認証のエラーの上限を設定し、設定値を超えて認証に失敗したユーザはアクセスできないようにします。

グループ設定 .... ユーザをグループに分けて登録・管理することができます。

ユーザ設定

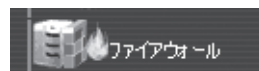
Express5800/SG300を利用したユーザ管理では、以下のような設定・管理を行うことができます。

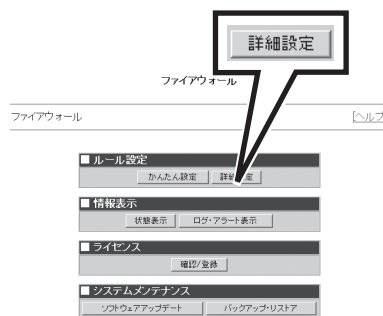
- ユーザ情報の確認
  Express5800/SG300が管理するユーザ情報を表示します。
- CSVファイルを経由したユーザの一括登録
  CSVファイルに記録したユーザ情報を読み込んで登録します。
- ユーザの個別追加
  ユーザを個別に登録します。
- ユーザ情報の削除
  登録したユーザ情報を削除します。
- ユーザ情報の更新
  登録済みのユーザ情報の内容を修正します。
- ユーザ情報のCSVファイルへの出力
  登録されているユーザ情報をCSVファイルに出力します。

ユーザ情報の確認

登録されているユーザ情報を確認することができます。

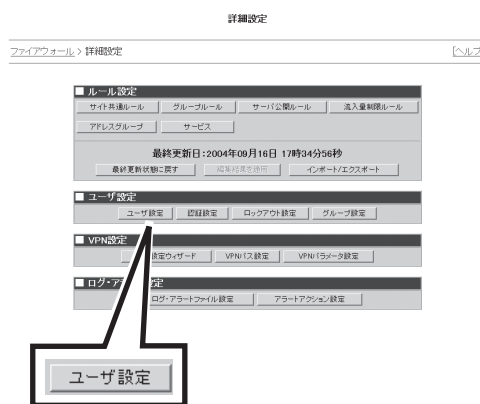
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

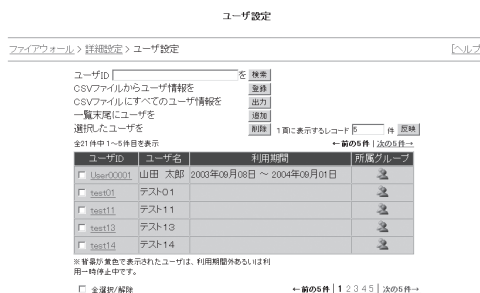
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。

   ユーザ情報一覧画面が表示されます。表示される内容は以下の通りです。

   - ユーザID
     登録されているユーザIDです。
   - ユーザ名
     登録されているユーザの名前です。
   - 利用期間
     利用可能な期間です。
   - 所属グループ
     アイコンをクリックするとグループの詳細情報を確認することができます。

ユーザ情報の一覧において、背景が黄色のユーザは、利用できないユーザであることを表しています。利用できないユーザとは、利用期間外となっているか、利用一時停止となっているユーザを指します。

詳細設定メニュー画面

ユーザ情報一覧画面

ヒント

- ユーザIDからユーザ情報を検索するには、ユーザ情報をテキストボックスに入力し[検索]をクリックします。指定したユーザIDのユーザが表示されます。
- 「1頁に表示するレコード」の入力フィールドに件数を入力し、[反映]をクリックすると、その指定した件数でユーザ情報を一覧表示します。

ユーザ情報一覧画面

CSVファイルを経由したユーザの一括登録

あらかじめユーザ情報をCSVファイルで作成しておけば、CSVファイルを読み込ませることでユーザを一括登録することができます。

作成するCSVファイルは以下のようなフォーマットで作成します。これ以外のフォーマットでは、正しく読み込むことができません。

ユーザID,認証方式,パスワード,システム情報,システム情報,利用一時停止フラグ,システム情報,利用開始年月日,利用停止年月日,ユーザ名,備考

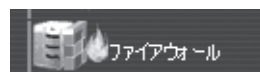
重要 **データの途中に不要なスペースなどは入れないでください。不要なスペースが入っていると正しく読み込めない場合があります。**

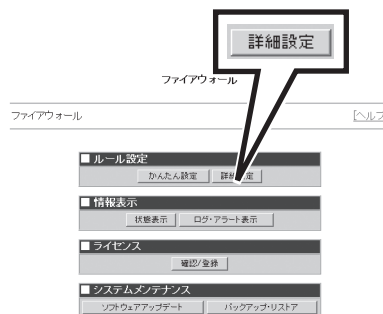
カラム	項目	入力規則	必須/任意
1	ユーザID	最大で256バイトまでの英数文字列、ハイフン（-）、アンダースコア（_）、アットマーク（@）、ピリオド（.）が使用できます。	必須
2	認証方式	現在はpasswordに固定です。	必須
3	パスワード	6バイト以上256バイト以内の英数文字列で指定します。 平分でパスワードを登録するときは、パスワードのみを指定してください。ハッシュされたパスワードを指定する場合は、先頭に"{SHA1}"とつけて登録します。取得したCSVファイルでは、ハッシュされたパスワードが指定されます。	必須
4	システム情報	空白を指定してください。 取得したCSVファイルを利用する場合は、編集しないで下さい。	任意
5	システム情報	空白を指定してください。 取得したCSVファイルを利用する場合は、編集しないで下さい。	任意
6	利用一時停止フラグ	0は利用可、1は利用不可です。 値が1のときはユーザ認証に失敗します。省略した場合は利用可（0を指定した場合と同じ）となります。	任意

カラム	項目	入力規則	必須/任意
7	システム情報	空白を指定してください。 取得したCSVファイルを利用する場合は、編集しないで下さい。	任意
8	利用開始年月日	YYYY/MM/DD形式で入力してください。 省略した場合は利用開始制限無しとなります。	任意
9	利用停止年月日	YYYY/MM/DD形式で入力してください。 省略した場合は利用停止制限無しとなります。	任意
10	ユーザ名	最大で128バイトまで指定できます。 カンマ(,)、ダブルクォーテーション(")、改行は使用できません。	必須
11	備考	最大で2048バイトまで指定できます。 カンマ(,)、ダブルクォーテーション(")は使用できません。	任意

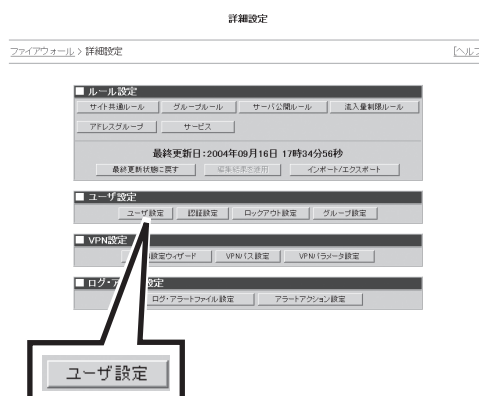
重要 **読み込むCSVファイルは、ファイアウォールが動作している機器上ではなく、Management Consoleを表示している管理クライアント上に保存してください。**

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

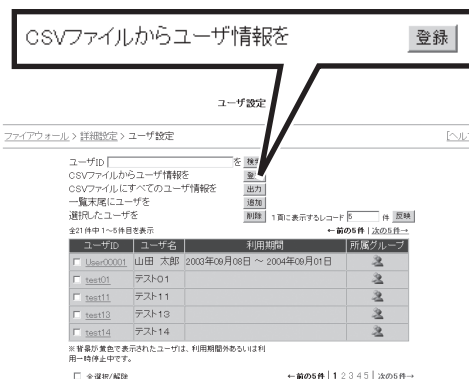
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。

   ユーザ情報一覧画面が表示されます。

詳細設定メニュー画面

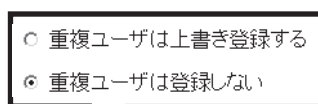
4. 「CSVファイルからユーザ情報を『登録』」をクリックする。

CSVファイル入力画面が表示されます。

5. テキストボックス内に直接ファイル名を入力するか、[参照]をクリックし、管理クライアントに保存されているファイルの中から該当ファイルを指定する。ファイルを指定したら[ファイル内容確認]をクリックする。

指定されたファイル内容が解析され、CSVファイル入力候補一覧画面が表示されます。

CSVファイル入力画面

6. CSVファイルと既に登録されたユーザ情報の中に重複データがある場合は、「重複ユーザは上書き登録する」または「重複ユーザは登録しない」のどちらかのラジオボタンをクリックする。

背景が黄色のユーザ情報は、CSVファイルの解析に失敗したレコードであることを示します。このレコードのデータは、ユーザ情報登録の対象とはしません。

7. [登録]をクリックする。

CSVファイル入力結果画面が表示されます。

[キャンセル]をクリックすると、CSVファイル入力画面に戻ります。

CSVファイル入力候補一覧画面

8. CSVファイル入力結果画面を確認し、[ユーザ設定に戻る]をクリックする。

> ✔ チェック
>
> - 背景が黄色で色づけされたユーザ情報は、登録に失敗したレコードであることを示します。
> - 背景が緑色で色づけされたユーザ情報は、すでに登録されていたレコードのため、登録を行わなかったことを示します。

ユーザ情報一覧画面に戻ります。このとき、新しく登録されたユーザ情報が一覧に反映された形で表示されます。

CSVファイル入力結果画面

ユーザの個別追加

ユーザ情報を個別に追加することができます。

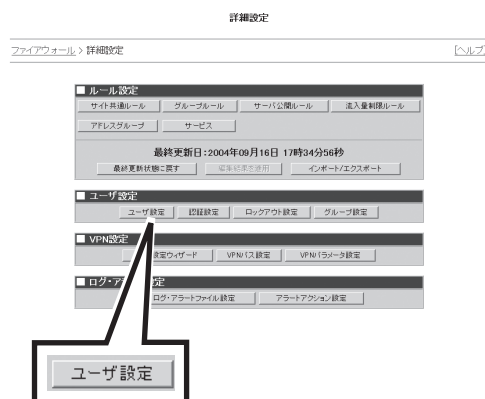
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

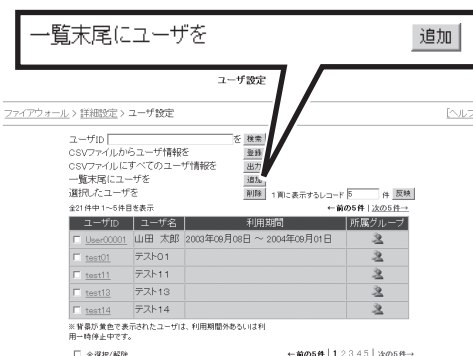
   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から〔ユーザ設定〕をクリックする。

   ユーザ情報一覧画面が表示されます。

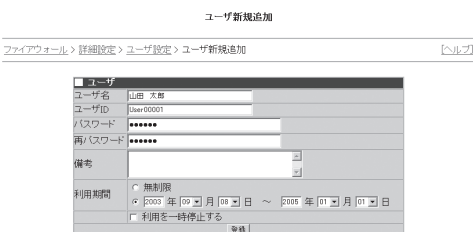
詳細設定メニュー画面

4. 「一覧末尾にユーザを『追加』」をクリックする。

   ユーザ情報追加画面が表示されます。

ユーザ情報一覧画面

5. ユーザ情報追加画面に表示される各項目を入力する。

ユーザ情報追加画面

   - ユーザ名（必須項目）
     追加するユーザを表す名称を入力します。最大で128バイトまでの任意の文字列を受け付けます。ただし、二重引用符(")とカンマ(,)を含めることはできません。
   - ユーザID（必須項目）
     追加するユーザを一意に表すIDを入力します。最大で256バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)、アットマーク(@)、ピリオド(.)を受け付けます。ただし、二重引用符(")とカンマ(,)を含めることはできません。すでに同じユーザIDの情報が登録されている場合には、登録に失敗します。
   - パスワード（必須項目）
     追加するユーザのパスワードを入力します。6バイトから256バイトまでの英数文字列を受け付けます。
   - 再パスワード（必須項目）
     追加するユーザのパスワードをもう一度入力します。

- 備考
  追加するユーザに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

- 利用期間
  追加するユーザの利用期間を限定するか、無制限にするかを選択します。利用期間外のときには、追加するユーザはログインできません。

- 利用を一時停止する
  運用上の理由などにより、追加するユーザの利用を一時停止したい場合、このチェックボックスにチェックをつけます。

6. ［登録］をクリックする。

   ユーザ情報追加結果画面が表示されます。

ユーザ情報の登録内容が入力規則に違反している場合は、エラー内容を示す画面が表示されます。

ユーザ情報追加画面

7. 所属グループを設定する場合は、［所属グループ設定へ］をクリックする。所属グループ設定画面が表示されるので、所属グループ一覧から所属するグループのチェックボックスをチェックし、［登録］をクリックする。

   所属グループ設定結果画面が表示されます。

ユーザ情報追加結果画面

8. 所属グループを設定しない場合は、ユーザ情報追加結果画面の［ユーザ設定に戻る］をクリックする。

   所属グループを設定した場合は、所属グループ登録結果画面の［ユーザ設定に戻る］をクリックする。
   ユーザ情報一覧画面に戻ります。このとき、新しく登録されたユーザ情報が一覧に反映された形で表示されます。

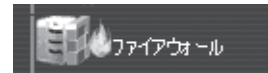
所属グループを設定するには、あらかじめ「グループ設定」をする必要があります。「グループ設定」については、235ページを参照してください。

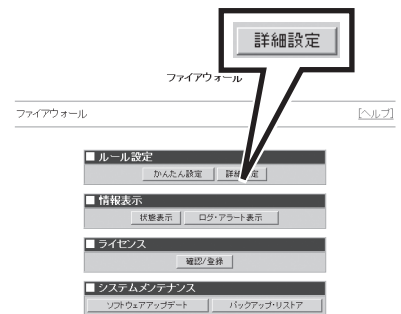
所属グループ設定結果画面

ユーザ情報の削除

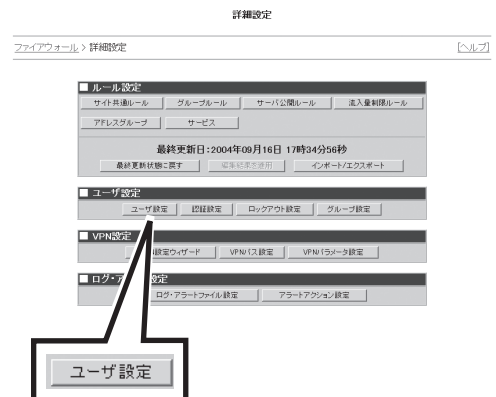
利用権限のなくなったユーザを削除することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。

   ユーザ情報一覧画面が表示されます。

詳細設定メニュー画面

4. 削除したいユーザのチェックボックスにチェックをつけ、「選択したユーザを『削除』」をクリックする。

ユーザ情報一覧画面

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

ヒント

[キャンセル]をクリックすると、削除されずにユーザ情報一覧画面に戻ります。

ユーザ情報が削除され、ユーザ一括削除結果画面が表示されます。

チェック

背景が黄色のユーザ情報は、削除に失敗したレコードであることを示します。

6. [ユーザ設定に戻る]をクリックする。

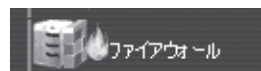
ユーザ情報一覧画面に戻ります。このとき、削除したユーザ情報は一覧に表示されません。

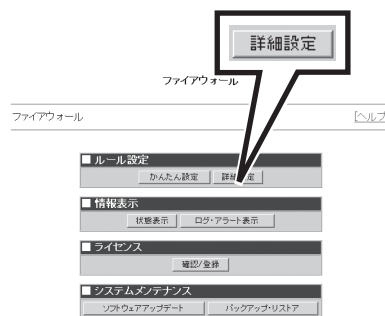
ユーザ一括削除結果画面

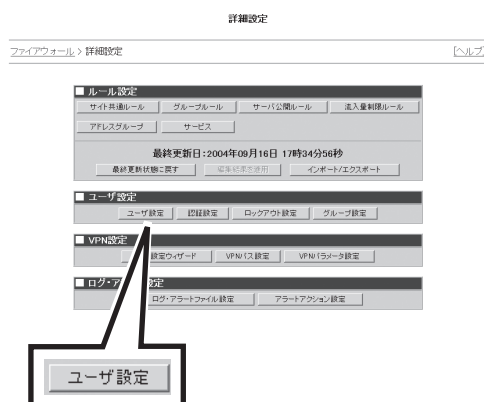
ユーザ情報の更新

ユーザ情報に変更があった場合、変更のあった項目のみ更新することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。

   ユーザ情報一覧画面が表示されます。

詳細設定メニュー画面

4. 情報を更新したいユーザのIDをクリックする。

   ユーザ情報更新画面が表示されます。

ユーザ情報一覧画面

5. ユーザ情報更新画面で更新したい項目を入力する。

ユーザ情報更新画面

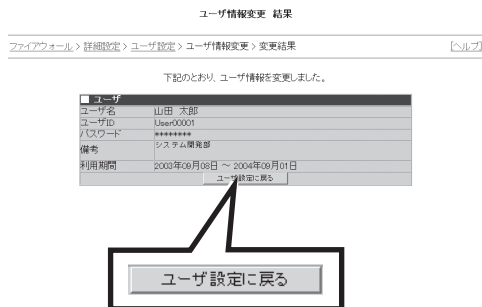
   - ユーザ名
     ユーザを表す名称を入力します。最大で128バイトまでの任意の文字列を受け付けます。ただし、二重引用符(")とカンマ(,)を含めることはできません。
   - ユーザID
     変更することはできません。
   - パスワード
     ユーザのパスワードを入力します。6バイトから256バイトまでの英数文字列を受け付けます。空白の場合、すでに登録されているパスワードが適用されます。
   - 再パスワード
     ユーザのパスワードをもう一度入力します。空白の場合、すでに登録されているパスワードが適用されます。
   - 備考
     ユーザに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。
   - 利用期間
     ユーザの利用期間を限定するか、無制限にするかを選択します。利用期間外のときには、ユーザはログインできません。
   - 利用を一時停止する
     運用上の理由などにより、ユーザの利用を一時停止したい場合、このチェックボックスにチェックをつけます。

6. [更新]をクリックする。

ユーザ情報更新結果画面が表示されます。

ユーザ情報の登録内容が入力規則に違反している場合は、エラー内容を示す画面が表示されます。

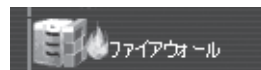
7. [ユーザ設定に戻る]をクリックする。

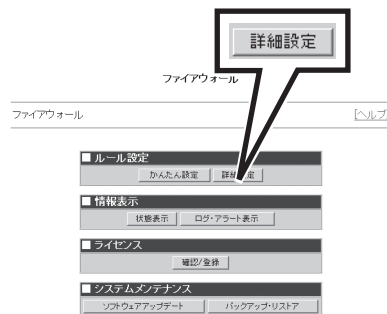
ユーザ情報一覧画面に戻ります。このとき、更新したユーザ情報が一覧に反映された形で表示されます。

ユーザ情報更新結果画面

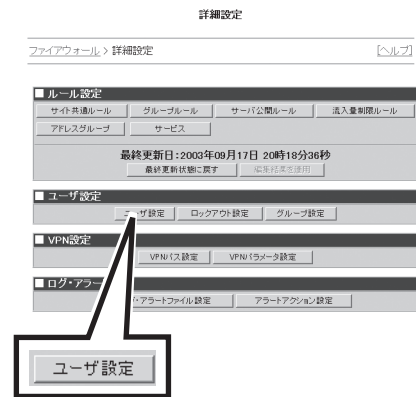
ユーザ情報のCSVファイルへの出力

Express5800/SG300が管理しているユーザ情報をCSVファイルに出力することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

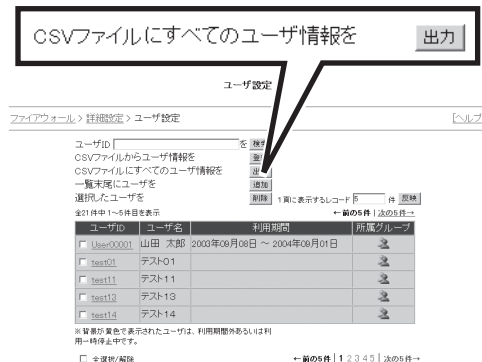
ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から〔ユーザ設定〕をクリックする。

ユーザ情報一覧画面が表示されます。

詳細設定メニュー画面

4. 「CSVファイルにすべてのユーザ情報を『出力』」をクリックする。

ファイル保存先指定画面が表示されます。

ユーザ情報一覧画面

5. ファイル名と保存先を指定し、〔保存〕をクリックする。

管理クライアント上に以下の形式でCSVファイルが保存されます。

カラム	項　目
1	ユーザID
2	認証方式
3	パスワード
4	システム情報
5	システム情報
6	利用一時停止フラグ
7	システム情報
8	利用開始年月日
9	利用停止年月日
10	ユーザ名
11	備考

出力に失敗した場合は、エラー内容を示す画面が表示されます。

認証設定

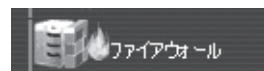
外部ネットワークから内部ネットワークに存在する端末にアクセスするときや、内部ネットワークから外部ネットワークに存在する端末にアクセスするときは、ファイアウォールとなるExpress5800/SG300を介して通信を行います。このとき、ユーザ認証によりユーザごとに使用する通信を許可することができます。ユーザ認証の利用の設定では、ユーザ認証を利用するかどうかを設定します。

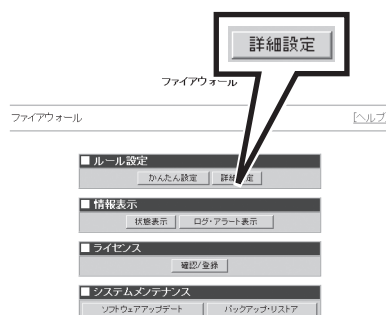
- ユーザの認証は、「ユーザ設定」で登録したユーザID、パスワードにより行います。また、認証を行ったユーザごとに通信の許可を行う場合は、ユーザを「グループ設定」でユーザグループに所属させ、該当ユーザグループの「グループルール」を設定する必要があります。
- 認証設定は、かんたん設定ウィザードからも設定することができます。ここで認証設定を更新すると、かんたん設定ウィザードで設定した認証設定も更新されます。

重要

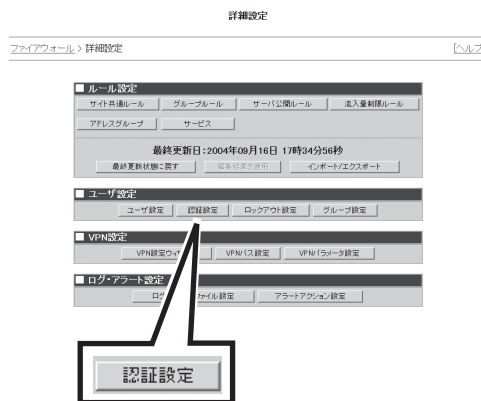
リモートアクセスVPNを利用する場合は、「ユーザ認証を利用する」に設定してください。認証の受付は「すべてのネットワークから許可する」に設定してください。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[認証設定]をクリックする。

   ユーザ認証設定画面が表示されます。

詳細設定メニュー画面

4. ユーザ認証の利用の有無を選択する。

●ユーザ認証を利用しない

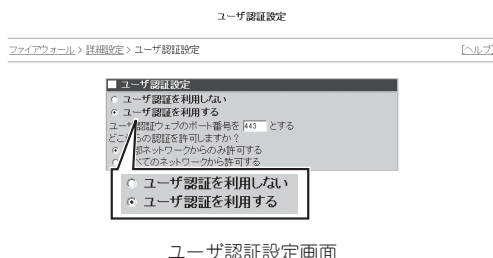
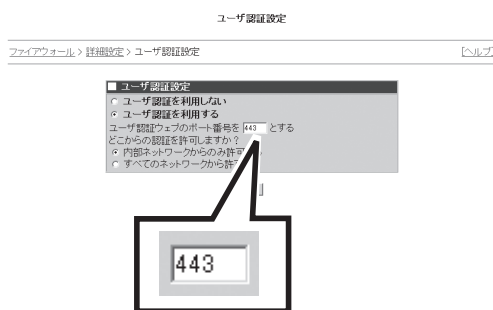
ユーザ認証を利用しない場合は、このラジオボタンをクリックし、手順7に進みます。

●ユーザ認証を利用する

ユーザ認証を利用する場合は、このラジオボタンをクリックし、手順5に進みます。

ユーザ認証設定画面

5. ユーザ認証ウェブのポート番号を指定する。

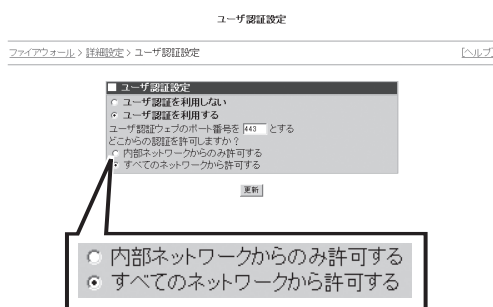
デフォルトでは「443」に設定されています。通常変更する必要はありません。

ユーザ認証設定画面

6. ユーザ認証の受付を設定する。

●内部ネットワークからのみ許可する

ユーザ認証のためのアクセスを、内部ネットワークからのみ受付けます。

●すべてのネットワークから許可する

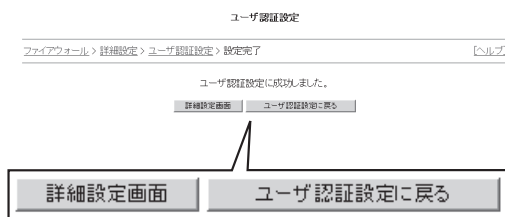
ユーザ認証のためのアクセスを、どこからでも受け付けます。

ユーザ認証の受付画面

7. ［更新］をクリックする。

ユーザ認証設定完了画面が表示されます。

8. 画面に表示されているいずれかのボタンをクリックする。

［詳細設定画面］をクリックすると詳細設定画面が表示されます。

［ユーザ認証設定に戻る］をクリックすると設定が反映されたユーザ認証設定画面が表示されます。

ユーザ認証設定完了画面

ロックアウト設定

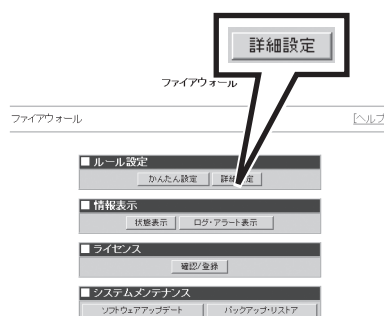
複数回に渡りユーザ認証に失敗したユーザについて、一定期間そのユーザをロックアウトすることができます。

ロックアウトとは、繰り返し認証に失敗すると、一定時間そのユーザ名でログインすることを無条件に禁止し、その間は正しいパスワードを入力してもログインさせせない仕組みです。本機能により、パスワードを繰り返し入力することによって、正しいパスワードを特定し、認証を通過しようとする攻撃を防ぐことが可能です。

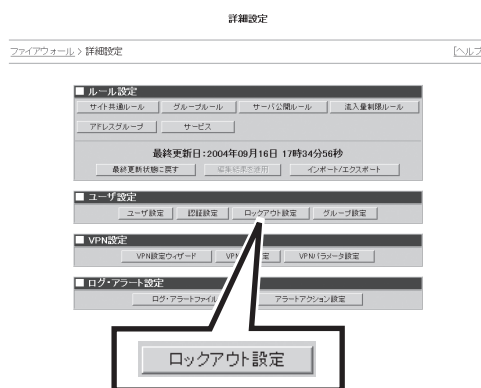
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[ロックアウト設定]をクリックする。

   ロックアウト設定画面が表示されます。

詳細設定メニュー画面

4. 画面に従い認証失敗をカウントする時間（秒）、ロックアウトするまでの回数、ロックアウトされたユーザによるログイン不能な時間（秒）を設定する。

ロックアウト設定画面

> ヒント
>
> [フォームのデータを元に戻す]をクリックすると、変更前の値に戻ります。

5. ［適用］をクリックする。

入力したロックアウト設定の内容でロックアウト機能を適用され、ロックアウト設定完了画面が表示されます。

> ヒント
>
> [ロックアウトの解除]をクリックすると、ロックアウト中の全ユーザのロックアウトを解除します。クリックすると確認画面が表示されるので、ロックアウトを解除する場合は[OK]をクリックします。解除が完了すると、解除完了画面が表示されます。

6. ［ロックアウト設定に戻る］をクリックする。

ロックアウト設定完了
ファイアウォール > 詳細設定 > ロックアウト設定 > ロックアウト設定完了
ロックアウト設定に成功しました。
ロックアウト設定に戻る
ロックアウト設定に戻る

グループ設定

Express5800/SG300を利用したユーザ管理では、グループを作成しユーザをグループ分けして管理することができます。グループ設定では、以下のような操作を行えます。

- グループ情報の確認
  現在登録されているグループ情報を確認することができます。
- グループ情報の追加
  グループ情報を新規に追加します。
- グループ情報の削除
  登録したグループ情報を削除します。
- グループ情報の更新
  登録したグループ情報の内容を変更します。

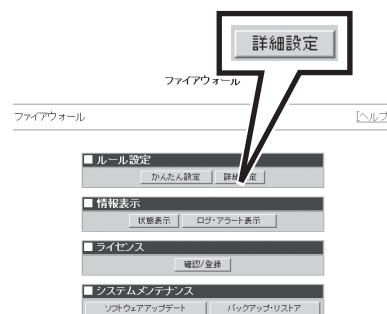
グループ情報の確認

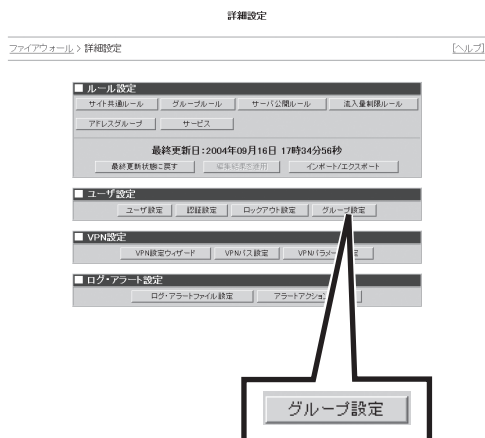
登録されているグループ情報を確認することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

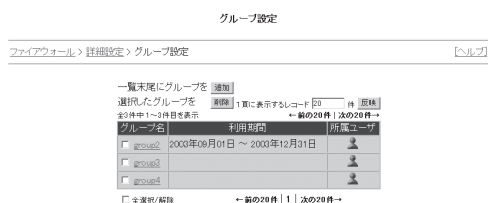
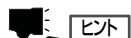
   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

詳細設定メニュー画面

グループ情報一覧画面が表示されます。表示される内容は以下の通りです。

グループ情報一覧画面

- グループ名
  登録されているグループの名称です。
- 利用期間
  利用可能な期間です。
- 所属ユーザ
  アイコンをクリックするとユーザの情報を確認することができます。

ヒント

「1頁に表示するレコード」の入力フィールドに件数を入力し、[反映]をクリックすると、その指定した件数でグループ情報を一覧表示します。

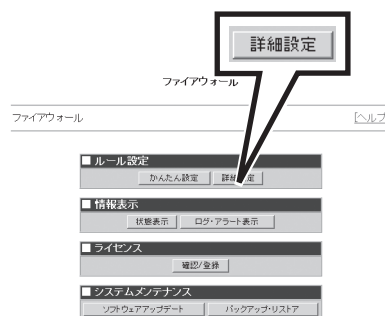
グループ情報の追加

グループ情報を新規に作成し、追加することができます。

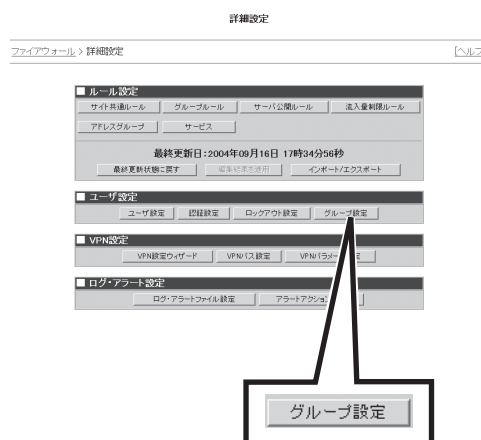
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

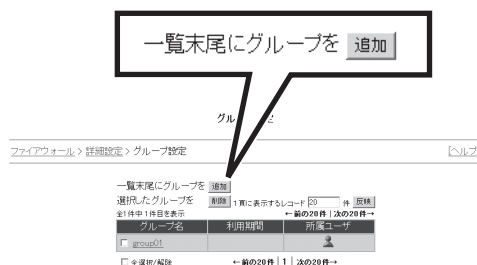
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

   グループ情報一覧画面が表示されます。

詳細設定メニュー画面

4. 「一覧末尾にグループを『追加』」をクリックする。

   グループ情報追加画面が表示されます。

グループ情報一覧画面

5. グループ情報追加画面に表示される各項目を入力する。

グループ情報追加画面

- グループ名(必須項目)
  追加するグループを表す名称を入力します。最大で256バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。既に同じ名前のグループ名がある場合には登録に失敗します。
- 利用期間
  追加するグループの利用期間を限定するか、無制限にするかを選択します。利用期間外のときには、追加するグループに対応したグループルールの適用はされません。
- 備考
  追加するグループに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

6. [登録]をクリックする。

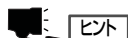
   グループ情報追加結果画面が表示されます。

グループ情報追加画面

7. 所属ユーザを設定する場合は、[所属ユーザ設定へ]をクリックする。所属ユーザ設定画面が表示されるので、ユーザIDから所属させるユーザのチェックボックスをチェックし、[更新]をクリックする。

   所属ユーザ設定結果画面が表示されます。

グループ情報追加結果画面

ヒント

グループに所属するユーザを設定するには、あらかじめ「ユーザ設定」をする必要があります。「ユーザ設定」については、217ページを参照してください。

8. 所属ユーザ設定結果画面の[グループ設定に戻る]をクリックする。

グループ情報一覧画面に戻ります。このとき、新しく登録されたグループ情報が一覧に反映された形で表示されます。

所属ユーザ設定結果画面

グループ情報の削除

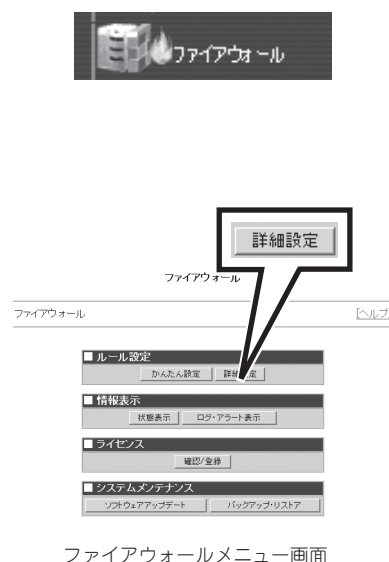
不要になったグループを削除することができます。

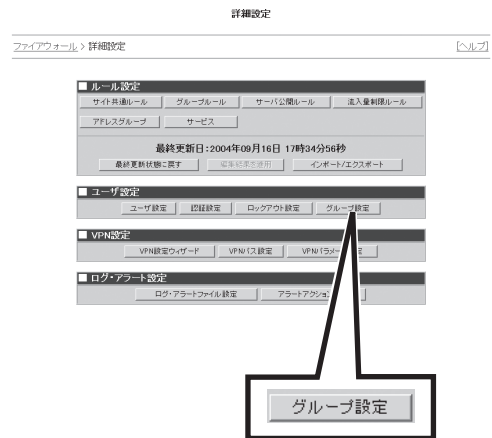
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

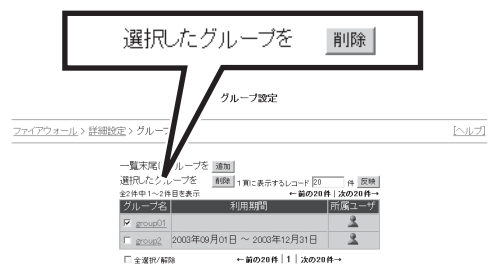
ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

   グループ情報一覧画面が表示されます。

詳細設定メニュー画面

4. 削除したいグループ名のチェックボックスにチェックをつけ、「選択したグループを『削除』」をクリックする。

グループ情報一覧画面

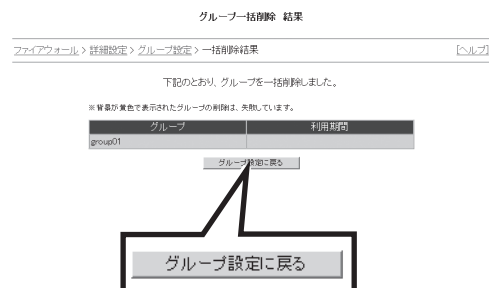
5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

> ヒント
>
> [キャンセル]をクリックすると、削除されずにグループ情報一覧画面に戻ります。

グループ情報が削除され、グループ一括削除結果画面が表示されます。

> チェック
>
> 背景が黄色のグループ情報は、削除に失敗したレコードであることを示します。

6. [グループ設定に戻る]をクリックする。

   グループ情報一覧画面に戻ります。このとき、削除したグループ情報は一覧に表示されません。

グループ一括削除結果画面

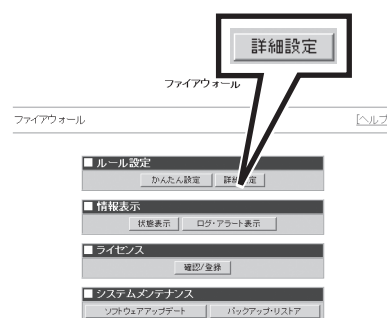
グループ情報の更新

グループ情報に変更があった場合、変更のあった項目のみ更新することができます。

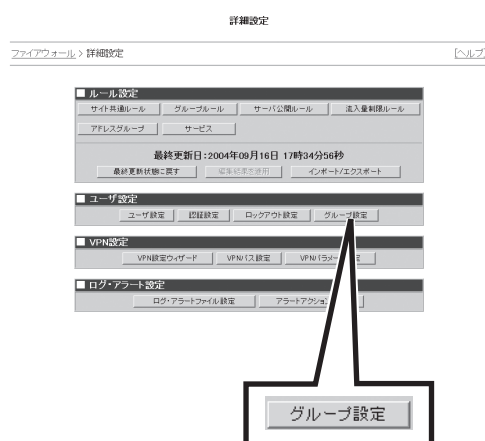
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

   グループ情報一覧画面が表示されます。

詳細設定メニュー画面

4. 情報を更新したいグループ名をクリックする。

   グループ情報更新画面が表示されます。

グループ情報一覧画面

5. グループ情報更新画面で更新したい項目を入力する。

グループ情報更新画面

- グループ名
  変更することはできません。
- 利用期間
  グループの利用期間を限定するか、無制限にするかを選択します。利用期間外のときには、グループに対応したグループルールの適用はされません。
- 備考
  グループに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

6. ［更新］をクリックする。

   グループ情報更新結果画面が表示されます。

7. ［グループ設定に戻る］をクリックする。

   グループ情報一覧画面に戻ります。このとき、更新したグループ情報が一覧に反映された形で表示されます。

8. 所属ユーザを更新する場合は、グループ情報一覧画面に表示される所属ユーザ情報のアイコンをクリックする。

   所属ユーザ設定画面が表示されます。

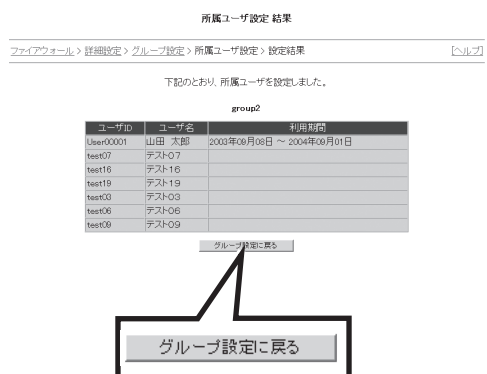
グループ情報一覧画面

9. ユーザIDから所属させるユーザのチェックボックスをチェックし、[更新]をクリックする。

所属ユーザ設定結果画面が表示されます。

所属ユーザ選択画面

10. [グループ設定に戻る]をクリックする。

グループ情報一覧画面に戻ります。このとき、変更したグループ情報が一覧に反映された形で表示されます。

所属ユーザ設定結果画面

VPN設定

Express5800/SG300はIPSecを利用したVPN通信を行うことができます。VPNパスの管理では、VPN通信を行うパスの設定や暗号通信方式の設定を行うことができます。ただし、VPNパスの中を通る通信が無条件に許可されることはないため、ここで定義したVPNパスの中を通る個々の通信については、別途フィルタリング設定が必要です。フィルタリング設定については、119ページの「サイト共通ルール」を参照してください。また、Express5800/SG300でVPN通信を行わず、他のVPN機器同士のVPN通信を通過させる場合は、「VPN設定」の対象となりません。この場合、「サイト共通ルール」で通信種別IPSecについて、フィルタリング設定を行う必要があります。
VPNパスの管理では、以下の項目の設定・管理を行います。

VPN設定ウィザード .... ウィザード形式でVPN設定を行うことができます。

VPNパス設定 .... VPNのパスを環境にあわせて自由に設定することができます。

VPNパラメータの設定 .... 同時に利用できるVPNトンネル数、トランスポート数の設定を行うことができます。

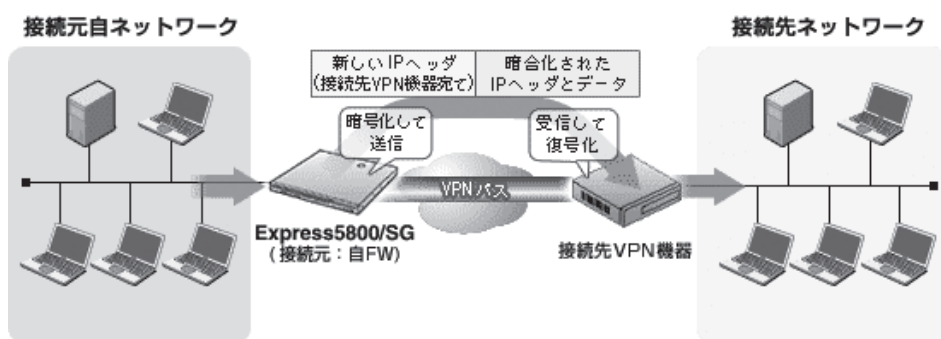
重要

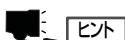
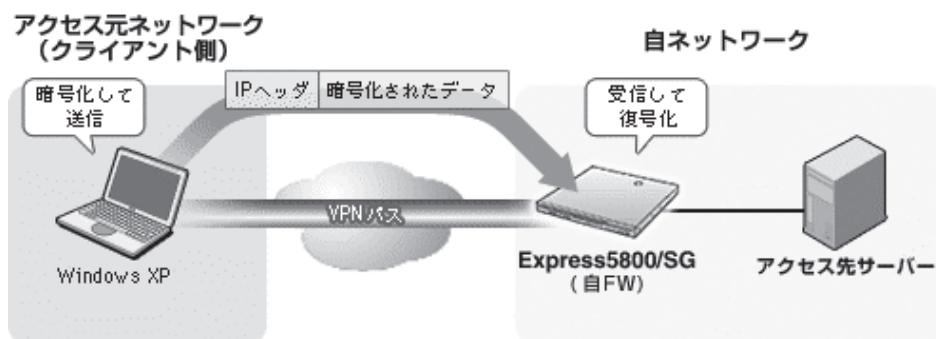
- **VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があると、VPN通信は行えません。**
- **VPN接続時に、停電などによりExpress5800/SG300の電源がOFFになると、相手側VPN機器にセキュリティアソシエーション(SA)が残るため、その残ったSAの有効時間が切れるまではVPN接続ができなくなります。**
- **Express5800/SG300自身がIPSecを使用せず、他サーバ間のIPSec通信の間に入る場合、ここでのVPN設定は不要です。ただし、サイト共通ルールで、サーバ間のIPSec通信を許可しておく必要があります。なお、このとき、かんたん設定で「アドレス変換(NAT/NAPT)を行う」設定をしていると、問題が起こることがあります(サーバ間のIPSecでAHを使用している場合)。**
- **Express5800/SG300でIPSecを使用し、接続先との経路上にファイアウォールが存在する場合、そのファイアウォールにおいて、IKEで使用するUDP 500番ポート、AH(プロトコル番号51)、ESP(プロトコル番号50)を通過できるように設定する必要があります。また、上記条件のもと、かんたん設定で「アドレス変換(NAT/NAPT)を行う」を設定し、AHを使用するように設定した場合、問題が起こることがあります(これはIPSecの仕様による制限です)。**

VPN設定ウィザード

複雑なVPN設定をウィザード形式で簡単に設定することができます。
VPNの接続方式としては、LANとLANをVPN接続するLAN間接続VPN(Gateway to Gateway VPN)と、リモート端末からVPN機器にアクセスして公開されたサーバにアクセスするリモートアクセスVPN(Host to Gateway VPN)があります。

● **LAN間接続VPN(Gateway to Gateway VPN):トンネルモード**

LAN間接続VPN(Gateway to Gateway VPN)では、自ネットワーク側LANのゲートウェイとなるExpress5800/SG300と通信相手側LANのGatewayとなるVPN通信機器間で暗号通信を行い、装置間にあたかも仮想的なトンネルがあるかのように接続を行います。この方式では、IPヘッダを含めたIPパケット全体を暗号化し、暗号化処理を行う装置のIPアドレスを宛先として通信します。

● **リモートアクセスVPN(Host to Gateway VPN):トランスポートモード**

リモートアクセスVPN(Host to Gateway VPN)では、通信を行う端末間で暗号通信を行います。IPヘッダの暗号化は行いません。

ヒント

VPN設定ウィザードでは、プリシェアードシークレットを利用した自動鍵交換方式のVPN通信の設定ができます。
事前共有鍵交換方式のVPN通信の設定は、「VPNパス設定」で追加することができます。

LAN間接続

LAN間接続VPNとは、2つのLANとLANのGatewayとなるVPN機器（Express5800/SG300等）の間にVPNパスを設定し、暗号化通信を行う方式です。
VPN設定ウィザードで設定したLAN間接続VPNは、自動鍵交換方式のトンネルモードとなります。

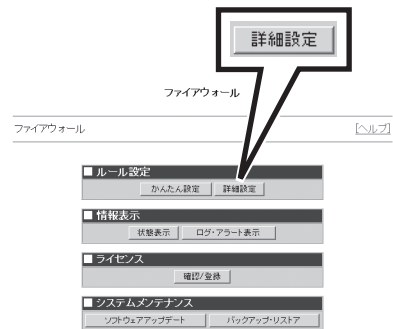
重要

- **VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があると、VPN通信は行えません。**
- **VPN接続時に、停電などによりSG300の電源がOFFになると、相手側VPN機器にセキュリティアソシエーション(SA)が残るため、その残ったSAの有効時間が切れるまではVPN接続ができなくなります。**

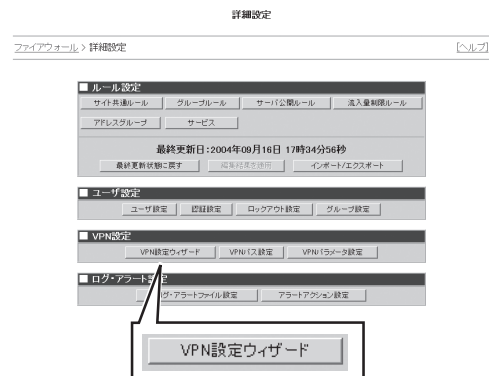
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

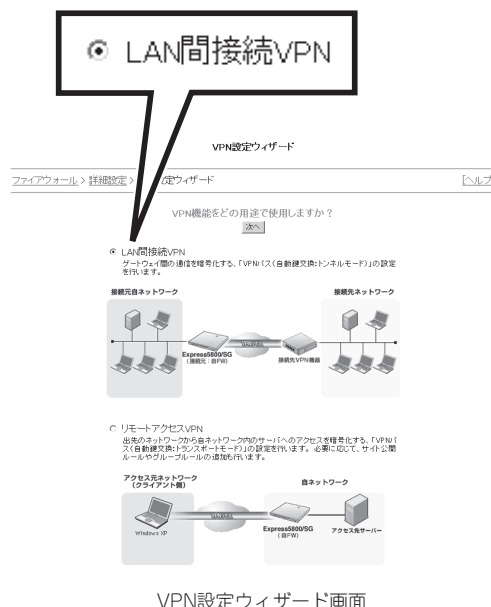
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPN設定ウィザード]をクリックする。

   VPN設定ウィザードが表示されます。

詳細設定メニュー画面

4. 「LAN間接続VPN」をクリックする。

VPN設定ウィザード画面

5. ［次へ］をクリックする。

LAN間接続VPN設定画面が表示され、LAN間接続VPNの設定に進みます。

6. LAN間接続VPNを設定する。

●接続先VPN機器のIPアドレス

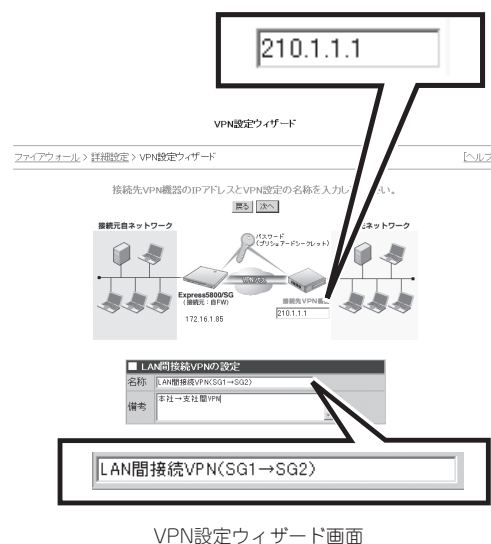
接続する先のVPN機器が外部に公開しているIPアドレスを設定します。

●名称

LAN間接続VPNを識別する任意の文字列を指定します。
名称は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

●備考

LAN間接続VPNに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。入力は任意です。

VPN設定ウィザード画面

7. ［次へ］をクリックする。

許可パス設定画面が表示され、許可パスの設定に進みます。

8. 許可パスを設定する。

●自ネットワークアドレス

自分側のネットワークアドレスを設定します。

●接続先ネットワークアドレス

LAN間接続VPNで接続する先のネットワークのアドレスを設定します。

●プリシェアードシークレット

あらかじめ、接続先と決めておいたプリシェアードシークレットを設定します。プリシェアードシークレットはVPNを使った暗号通信を実現するために必要なパスワードのようなものです。

VPN設定ウィザード画面

チェック

プリシェアードシークレットには必ず英数字を組み合わせた8文字以上500文字以内の文字列を設定してください。

9. ［次へ］をクリックする。

暗号化/認証アルゴリズム設定画面が表示され、接続先VPN機器の設定に進みます。

10. プルダウンメニューから「接続先VPN機器の種類」を選択する。

接続先VPN機器は、「Express5800/SG」、「IX2015」「Firewall-1」、「NetScreen」から選択することができます。

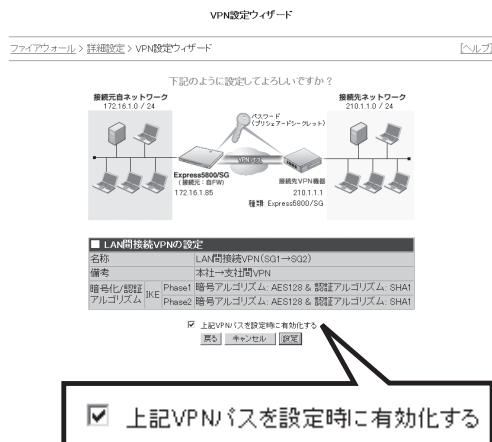
ヒント

- 接続先VPN機器を選択すると、自動的に適した暗号化アルゴリズムと認証アルゴリズムが設定されます。
- 表示される機器以外のVPN機器をご利用の場合は、「VPNパス設定」で暗号化アルゴリズムと認証アルゴリズムを変更することができます。

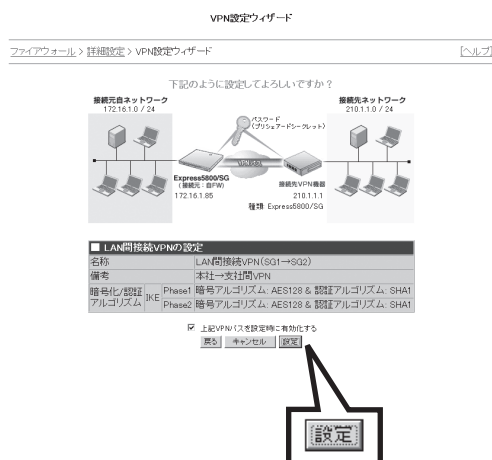
VPN設定ウィザード画面

11. ［次へ］をクリックする。

設定内容確認画面が表示されます。

12. 設定内容を確認する。設定した内容をすぐに適用するには、[上記VPNパスを設定時に有効にする]のチェックボックスにチェックする。

VPN設定ウィザード画面

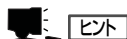
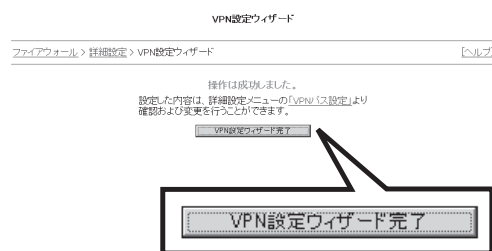
13. 問題がなければ[設定]をクリックする。

設定が誤っている場合は、[戻る]で設定画面に戻ることができるので、設定をやり直してください。[キャンセル]をクリックすると、これまでの設定内容が破棄されます。

VPN設定ウィザード画面

[設定]をクリックし、内容が正常に設定された場合は、結果画面が表示されます。

[VPN設定ウィザード完了]をクリックすると、詳細設定メニュー画面に戻ります。

VPN設定ウィザード画面

ヒント

ここで設定したVPNパスの内容は、[VPNパス設定]から、変更することができます。

リモートアクセスVPN

リモートアクセスVPNとは、ネットワークから離れた場所にある端末からネットワーク内のExpress5800/SG300の間にVPNパスを設定し、暗号化通信を行う方式です。このとき、サーバへのアクセス設定を行うことで、指定したサーバへのユーザからのアクセスを受け付けることができます。
リモートアクセスVPNを構築することにより、自宅や出張先からインターネット経由で企業内ネットワークへ安全にアクセスすることが可能になります。
VPN設定ウィザードで設定したリモートアクセスVPNは、自動鍵交換方式のトランスポートモードとなります。

重要

- **リモートアクセスVPN環境を構築するには、ユーザ認証が必須となります。そのため、VPN設定前の事前準備として、「かんたん設定」のユーザ認証の利用の設定または詳細設定メニューの「認証設定」よりユーザ認証が利用できるように設定しておく必要があります。「ユーザ認証」については、231ページを参照してください。**
- **VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があると、VPN通信は行えません。**
- **VPN接続時に、停電などによりExpress5800/SG300の電源がOFFになると、相手側端末にセキュリティアソシエーション(SA)が残るため、その残ったSAの有効時間が切れるまではVPN接続ができなくなります。**

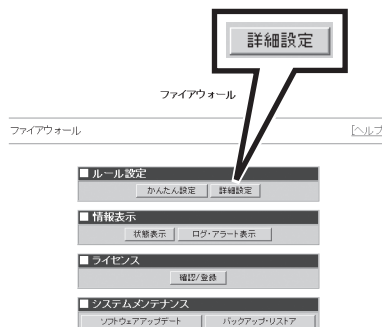
リモートアクセスVPNの設定

リモートアクセスVPNでは、クライアントアドレス(リモートからVPN通信で内部ネットワークにアクセスする端末のIPアドレス)を任意とするVPNパス(自動鍵交換：トランスポートモード)を1つ設定します。
複数のサーバのリモートアクセスを許可するには、そのVPNパス設定を利用してVPN設定ウィザードから公開するサーバのIPアドレスを指定します。公開するサーバごとに、グループが作成されます。
VPN設定ウィザードを利用した2回目以降の設定は、254ページの「アクセス先サーバが2台以上ある場合の設定について」を参照してください。

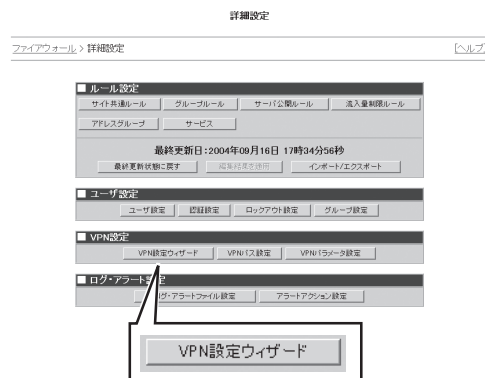
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

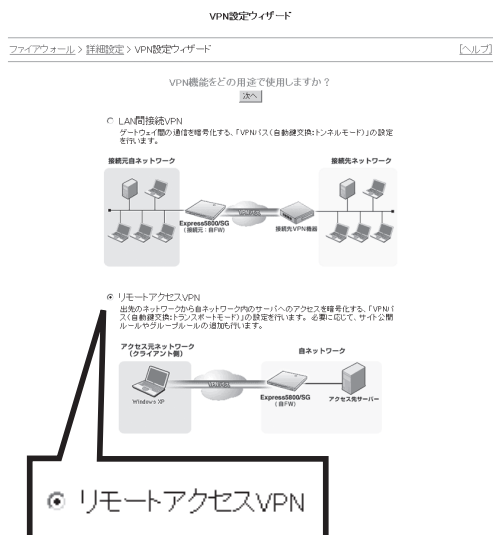
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPN設定ウィザード]をクリックする。

VPN設定ウィザードが表示されます。

詳細設定メニュー画面

4. 「リモートアクセスVPN」をクリックする。

VPN設定ウィザード画面

5. [次へ]をクリックする。

リモートアクセスVPN設定画面が表示され、リモートアクセスVPNの設定に進みます。

6. リモートアクセスVPNを設定する。

●名称

リモートアクセスVPNを識別する任意の文字列を指定します。
名称は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

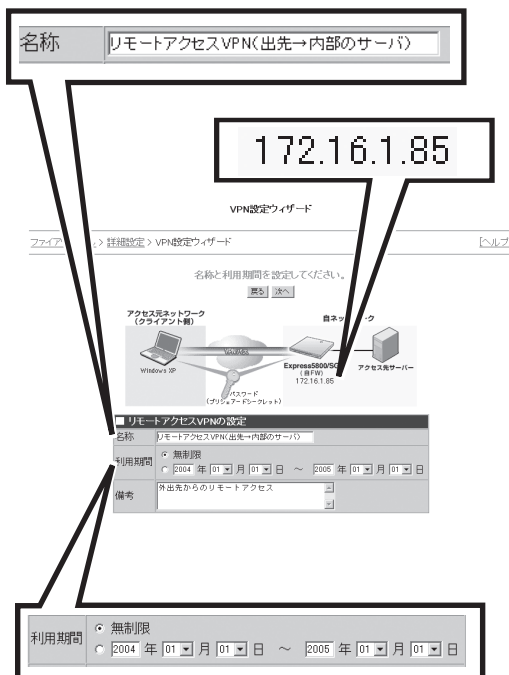
●利用期間

リモートアクセスVPNの利用期間を制限しない場合は「無制限」をクリックします。
期間を制限する場合は、プルダウンメニューを使って利用期間を指定します。

●備考

リモートアクセスVPNに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(“)およびカンマ(,)を含めることはできません。入力は任意です。

VPN設定ウィザード画面

チェック

名称には、既に設定した名称と同様の名称は設定することができません。

ヒント

「このVPNパスを利用するユーザのグループ」として、ここで設定した名称で新しくグループとグループルールが追加されます。グループへのユーザ登録は手順14で行うことができます。

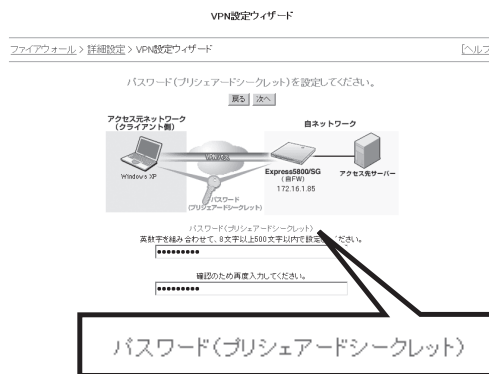
7. [次へ]をクリックする。

プリシェアードシークレット設定画面が表示され、プリシェアードシークレットの設定に進みます。

8. プリシェアードシークレットを設定する。

●プリシェアードシークレット

あらかじめ、接続先と決めておいたプリシェアードシークレットを設定します。プリシェアードシークレットはVPNを使った暗号通信を実現するために必要なパスワードのようなものです。

チェック

プリシェアードシークレットは必ず英数字を組み合わせた8文字以上500文字以内の文字列を設定してください。

VPN設定ウィザード画面

9. ［次へ］をクリックする。

アクセス先サーバ設定画面が表示され、リモート端末からVPN接続でアクセスするサーバの設定に進みます。

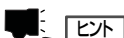
10. リモートからアクセスを許可するサーバを設定する。

VPN設定ウィザード画面

- アクセス先サーバの内部IPアドレス

  リモートからアクセスを許可するサーバの内部IPアドレスを設定します。

- アドレス変換の設定

  アドレス変換時のポート番号を設定します。外部ネットワークに公開するポート番号と対応する内部ポート番号を設定します。TCPとUDPをラジオボタンで指定することができます。

ヒント

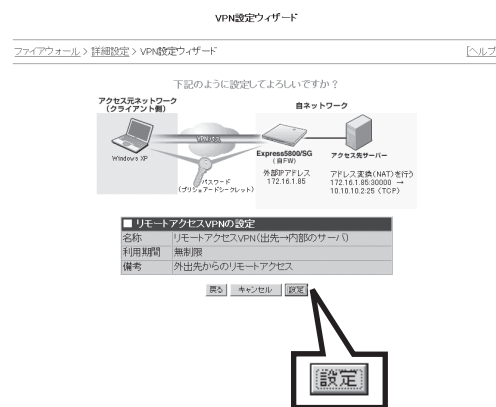
公開するIPアドレスやポート番号の変換については、「サーバ公開ルール」の設定内容に影響します。

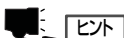
設定の途中で設定済みのサーバ公開ルールを確認したい場合は、画面下の説明文中の「既存の設定を確認する」をクリックしてください。

11. ［次へ］をクリックする。

設定内容確認画面が表示されます。

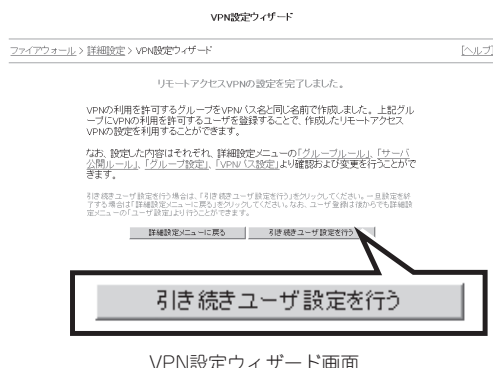
12. 設定内容を確認し、問題がなければ［設定］をクリックする。

設定が誤っている場合は、［戻る］で設定画面に戻ることができるので、設定をやり直してください。［キャンセル］をクリックすると、これまでの設定内容が破棄されます。

VPN設定ウィザード画面

［設定］をクリックし、内容が正常に設定された場合は、結果画面が表示されます。

ヒント

ここで設定した内容は、「グループルール」、「サーバ公開ルール」、「グループ設定」、「VPNパス設定」に影響します。また、各設定画面から変更することができます。

13. リモートからアクセスするユーザを設定する場合は、[引き続きユーザ設定を行う]をクリックする。

    ユーザ設定画面が表示されます。ユーザ設定については、217ページの「ユーザ設定」を参照してください。

VPN設定ウィザード画面

アクセス先サーバが2台以上ある場合の設定について

複数のサーバへのリモートアクセスを許可する場合は、VPN設定ウィザードから同じように設定します。ただし、2回目以降は、VPNパス(自動鍵交換：トランスポートモード)の設定は完了しているため、プリシェアードシークレットは設定する必要がありません。「名称」、「利用期間」、「アクセス先サーバのIPアドレス」、および「NAT設定」のみを設定します。プリシェアードシークレットを変更すると、その他のリモートアクセスVPNのプリシェアードシークレットも変更されますので注意してください。
なお、「名称」はすでに設定した名称と同じ名称は設定できません。同じものがある場合は、設定確認時に変更画面が表示されます。自動的に、設定した名称の末尾に「其の2」、「其の3」と番号が付与されますが、任意の文字列に変更することもできます。
ここでは、2回目以降のリモートアクセスVPNの設定について説明します。VPN設定ウィザードの表示以降から説明します。

1. VPN設定ウィザードで「リモートアクセスVPN」をクリックする。

2. [次へ]をクリックする。

    VPNパス設定画面が表示され、VPNパスの設定に進みます。

3. VPNパスを設定する。

    ●名称
    ●利用期間
    ●備考

4. [次へ]をクリックする。

    プリシェアードシークレット設定画面が表示され、プリシェアードシークレットの設定に進みます。

5. すでに設定しているVPNパス（自動鍵交換：トランスポートモード）と同様のプリシェアードシークレットを利用する場合は、入力せずに［次へ］をクリックする。変更する場合は、プリシェアードシークレットを入力する。

   アクセス先サーバ設定画面が表示され、リモート端末からVPN接続でアクセスするサーバの設定に進みます。

VPN設定ウィザード画面

6. リモートからアクセスを許可するサーバを設定する。

   ●アクセス先サーバの内部IPアドレス

   ●アドレス変換の設定

7. ［次へ］をクリックする。

   設定内容確認画面が表示されます。

8. 設定内容を確認し、問題がなければ［設定］をクリックする。

   「名称」がすでに設定した「名称」と重なっている場合は、名称変更画面が表示されます。自動的に設定した名称の末尾に「其の2」、「其の3」と番号が付与されますが、任意の文字列に変更することもできます。
   手順5でプリシェアードシークレットを入力した場合は、VPNパスの上書き確認画面が表示されます。

9. プリシェアードシークレットを上書きしてもよければ［はい］をクリックする。
   プリシェアードシークレットを上書きしない場合は、［パスワードを変更しないで設定］をクリックする。

10. 設定完了画面が表示される。リモートからアクセスするユーザを設定する場合は、［引き続きユーザ設定を行う］をクリックする。

    ユーザ設定画面が表示されます。ユーザ設定については、217ページの「ユーザ設定」を参照してください。

VPNパス設定

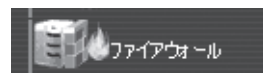
VPNパス設定では、VPN設定ウィザードで設定したVPNパスを変更したり、新たなVPNパスを追加したりすることができます。
VPNパス設定では、以下の項目を設定／管理します。

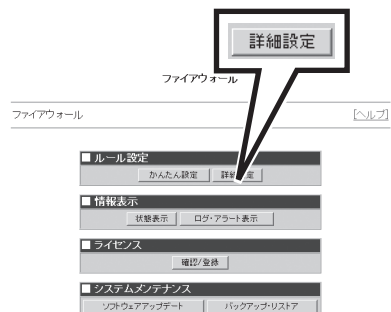
- VPNパスの確認
- VPNパスの追加（共有鍵交換）
- VPNパスの追加（自動鍵交換：トンネルモード）
- VPNパスの追加（自動鍵交換：トランスポートモード）
- VPNパスの削除
- VPNパスの更新

VPNパス確認

すでに設定したVPNパスはVPN情報一覧画面から確認することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

   VPNパス設定画面が表示されます。表示される内容は以下の通りです。

詳細設定メニュー画面

項目		説　明
パス番号		VPNパスの番号です。
VPNパス	接続先IPアドレス	VPN通信を行う相手のIPアドレスです。
	自IPアドレス	Express5800/SG300の外部ネットワークに接続したインタフェースに割り当てられたIPアドレスです。
許可パス	接続組み合わせ	VPN通信を行う相手先と自ネットワークの組み合わせです。 自動鍵交換方式のトランスポートモードでは表示されません。
モード		VPN通信を行うモードです。
鍵交換方式		鍵の交換方式です。

VPNパス設定画面

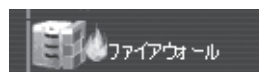
ヒント

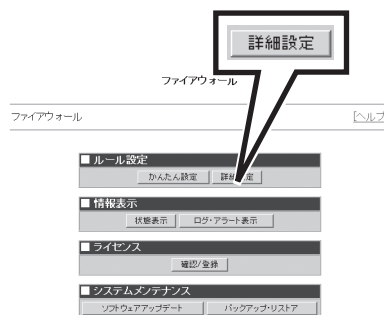
「1頁に表示するレコード」の入力フィールドに件数を入力し、[反映]をクリックすると、その指定した件数でVPNパスを一覧表示します。

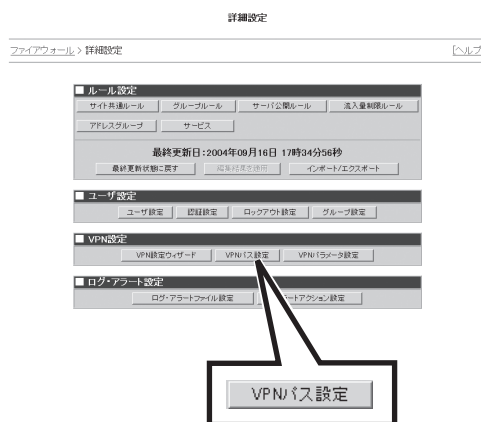
VPNパスの追加(共有鍵交換)

必要に応じてVPNパスを追加することができます。ここでは、共有鍵交換方式を利用したVPNパスの設定について説明します。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

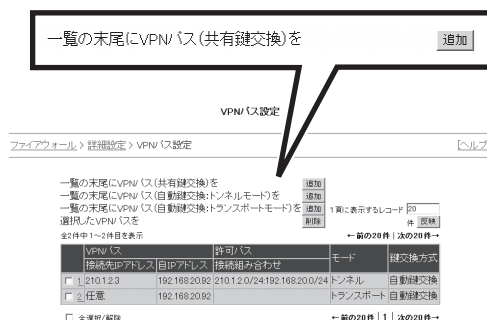
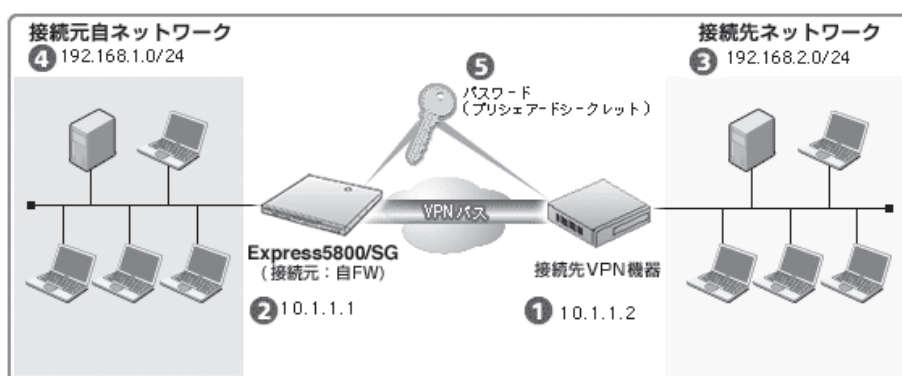
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

   VPNパス設定画面が表示されます。

詳細設定メニュー画面

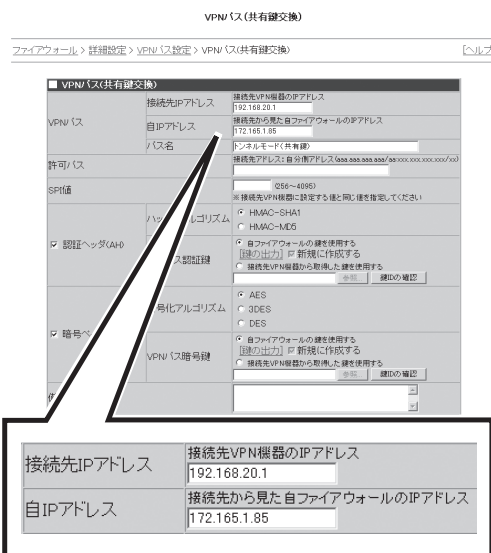
4. 「一覧の末尾にVPNパス(共有鍵交換)を『追加』」をクリックする。

VPNパス(共有鍵交換)画面が表示されます。

VPNパス設定画面

以降の各項目の設定手順では、VPN通信の概念を理解しやすくするために以下の図を用いて説明します。

5. VPNパスを設定する。

- 接続先IPアドレス
  VPNパスをはる接続先VPN機器が外部に公開しているIPアドレスを入力します(VPNパスの概念図の①)。
- 自IPアドレス
  VPNパスをはる接続先から参照することができる、Express5800/SG300の外部ネットワークにつなげたインタフェースのIPアドレスを入力します(VPNパスの概念図の②)。
- パス名
  VPNパスを識別する任意の文字列を指定します。VPNパス名は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

VPNパス(共有鍵交換)画面

ファイアウォール機能の設定方法

6. 許可パスを入力する。

VPNパスをはる接続先アドレス(VPNパスの概念図の③)と自分側のアドレス(VPNパスの概念図の④)との組みを入力します。「接続先IPアドレス/ネットマスク:自分側IPアドレス/ネットマスク」のように、ネットマスクを含めた形で指定します。

IPアドレスだけを指定したい場合にはネットマスクを32としてください。

VPNパス(共有鍵交換)画面

7. SPI値を入力する。

SPIとはトンネルを一意に特定するIDです。VPNによる暗号化通信を行う接続先との間で取り決めたSPI値を入力します。値の有効範囲は、256から4095までです。

VPNパス(共有鍵交換)画面

8. 認証ヘッダ(AH)を利用する場合、チェックボックスにチェックし、ハッシュアルゴリズムとVPNパス認証鍵の設定を行う。

VPNパス(共有鍵交換)画面

ヒント

AHはIPヘッダを含めたパケットの改ざん検知を行います。AHはハッシュアルゴリズムを使って送信データとVPNパス認証鍵から認証データを生成し、その認証データを送信データに付与して一緒に送ります。通信相手はデータを受信したとき、同様にハッシュアルゴリズムを使ってデータと認証鍵から認証データを生成し、送られてきた認証データと比較します。通信の途中で第三者がパケットの内容を改ざんした場合は、送信された認証データと受信者の生成した認証データが異なるため、改ざんの有無を検出することができます。

- ハッシュアルゴリズム
  HMAC-SHA1とHMAC-MD5から選択します。あらかじめ通信相手とアルゴリズムを決めておき、通信相手と同様のものを設定します。
- VPNパス認証鍵
  VPNパスの認証に使用する共有鍵を指定します(VPNパスの概念図の⑤)。
  共有鍵は自ファイアウォールと接続先VPN機器で同一の鍵を共有する必要があるため、どちらか一方のノードで鍵を生成し、生成した鍵データをもう一方のノードに転送して利用します。
  - 自ファイアウォールの鍵を使用する
    Express5800/SG300で作成した鍵を使用するときに選択し、[鍵の出力]をクリックして鍵データをファイルに出力します。鍵を新規に作る、または作り直す場合は、「新規に作成する」チェックボックスにチェックをしてから[鍵の出力]をクリックしてください。そのファイルを接続先VPN機器に渡して、VPNパス認証鍵として設定してください。
  - 接続先VPN機器から取得した鍵を使用する
    接続先のVPN機器で作成した鍵を使用するときに選択します。テキストボックスに、接続先VPN機器から出力した鍵ファイル名を指定します。ファイル名を直接入力するか、[参照]をクリックしてファイルを選択してください。
    鍵ファイル名を指定した後、[鍵IDの確認]をクリックすると、鍵IDの確認画面を別ウィンドウで表示します。

読み込む鍵ファイルは、ファイアウォールが動作している端末ではなく、Management Consoleを表示している管理クライアント上に保存してください。

9. 暗号化ペイロード(ESP)を利用する場合、チェックボックスにチェックし、暗号化アルゴリズムとVPNパス暗号鍵の設定を行う。

ヒント

ESPではVPNパス暗号鍵と暗号化アルゴリズムを使ってパケットを暗号化することで、通信の機密性を保証します。

VPNパス(共有鍵交換)画面

- 暗号化アルゴリズム
  暗号化アルゴリズムを、AES、3DES、DESから選択します。あらかじめ通信相手とアルゴリズムを決めておき、通信相手と同様のものを設定します。

- VPNパス暗号鍵
  暗号通信に使用する共有鍵を指定します(VPNパスの概念図の⑤)。
  自ファイアウォールと接続先VPN機器とで1つの鍵を共有する必要があります。したがって、どちらか一方で鍵を生成したらもう一方に同一の鍵データを渡し、渡された方は鍵データを読み込みます。

  ー 自ファイアウォールの鍵を使用する
  Express5800/SG300で作成した鍵を使用するときに選択し、[鍵の出力]をクリックして暗号鍵をファイルに出力します。鍵を新規に作る、または作り直す場合は、「新規に作成する」チェックボックスにチェックをしてから[鍵の出力]をクリックしてください。そのファイルを接続先VPN機器に渡して、VPNパス暗号鍵として設定してください。

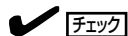
  ー 接続先VPN機器から取得した鍵を使用する
  接続先のVPN機器で作成した鍵を使用するときに選択します。入力フィールドに、接続先VPN機器から出力した鍵ファイル名を指定します。ファイル名を直接入力するか、[参照]をクリックしてファイルを選択してください。
  鍵ファイル名を指定した後、[鍵IDの確認]をクリックすると、鍵IDの確認画面を別ウィンドウに表示します。

読み込む鍵ファイルは、ファイアウォールが動作している端末ではなく、Management Consoleを表示している管理クライアント上に保存してください。

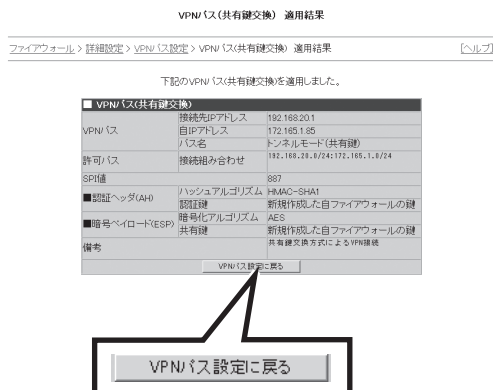
10. VPNパスに関する備考を入力する。

最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。入力は任意です。

11. [適用]をクリックする。

VPNパス(共有鍵交換)適用結果画面が表示されます。

登録に失敗した場合には、エラー内容を示す画面を表示します。

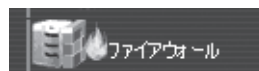
12. [VPNパス設定に戻る]をクリックする。

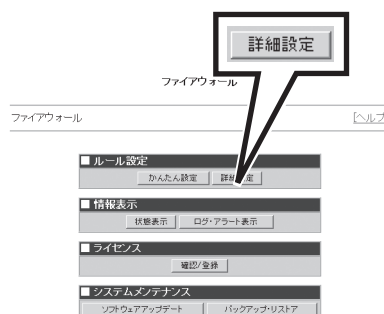
追加したVPNパスが反映されたVPNパス設定画面が表示されます。

VPNパス(共有鍵交換)適用結果画面

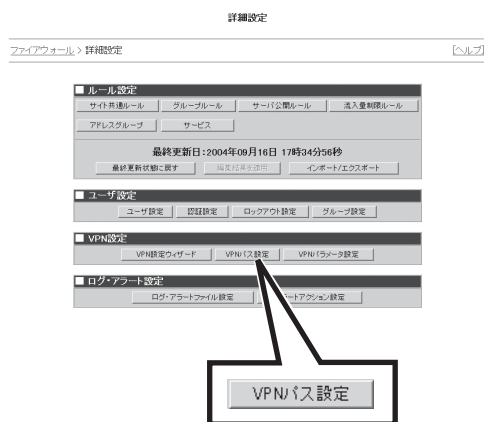
VPNパスの追加（自動鍵交換：トンネルモード）

必要に応じてVPNパスを追加することができます。ここでは、トンネルモードにおける自動鍵交換方式を利用したVPNパスの設定について説明します。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

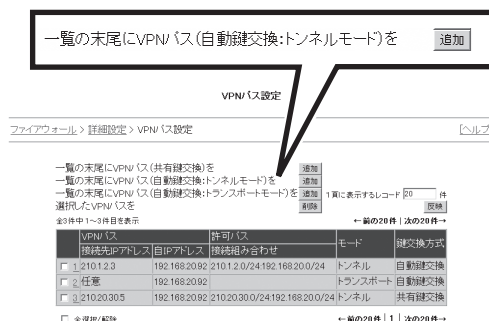
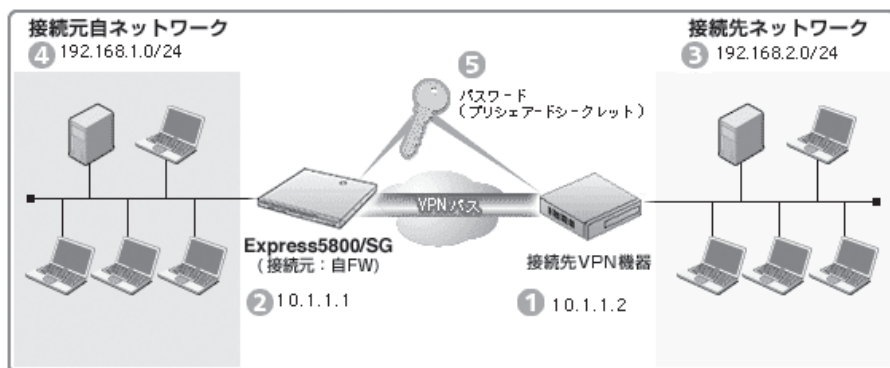
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

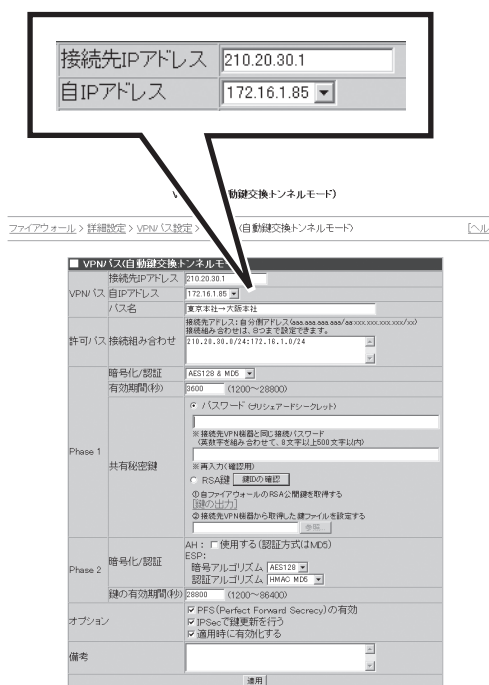
3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

   VPNパス設定画面が表示されます。

詳細設定メニュー画面

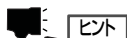
4. 「一覧の末尾にVPNパス（自動鍵交換：トンネルモード）を『追加』」をクリックする。

VPNパス（自動鍵交換：トンネルモード）画面が表示されます。

VPNパス設定画面

以降の各項目の設定手順では、VPN通信の概念を理解しやすくするために以下の図を用いて説明します。

5. VPNパスを設定する。

- 接続先IPアドレス
  VPNパスをはる接続先VPN機器が外部に公開しているIPアドレスを入力します（VPNパスの概念図の①）。
- 自IPアドレス
  VPNパスをはる接続先から参照することができる、Express5800/SG300の外部ネットワークにつなげたインタフェースのIPアドレスをプルダウンメニューから選択します（VPNパスの概念図の②）。
- パス名
  VPNパスを識別する任意の文字列を指定します。VPNパス名は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

VPNパス（自動鍵交換：トンネルモード）画面

6. 許可パスを入力する。

VPNパスをはる接続先アドレス(VPNパスの概念図の③)と自分側のアドレス(VPNパスの概念図の④)との組みを一行に一組ずつ入力します。「接続先IPアドレス/ネットマスク:自分側IPアドレス/ネットマスク」のように、ネットマスクを含めた形で指定します。

IPアドレスだけを指定したい場合にはネットマスクを32としてください。

VPNパス(自動鍵交換:トンネルモード)画面

7. Phase1の「暗号化/認証」、「有効期間」を設定する。

ヒント

自動鍵交換方式では、最初にIKEを使って通信相手を認証し、暗号化アルゴリズムと暗号鍵を決定します。事前にパスワードまたはRSA鍵を共有していることが条件になります。

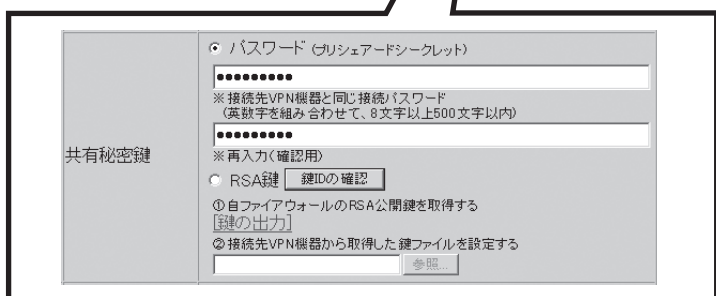
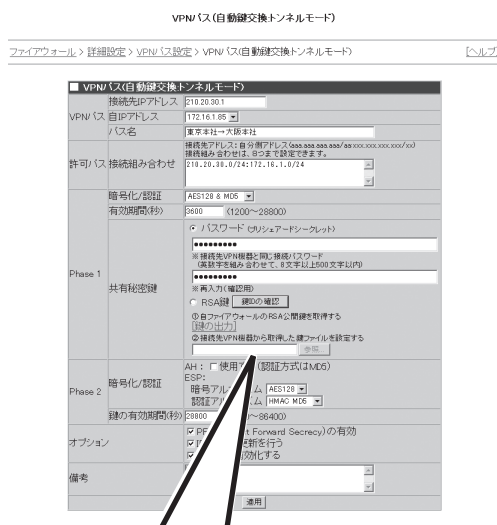
IKEでは、まずハッシュアルゴリズムとパスワード(またはRSA鍵)を使って通信相手双方の認証を行います。認証完了後、暗号通信を利用して鍵の元となる乱数データと暗号化アルゴリズムを通知しあい、実際の通信で使用する共通鍵(秘密鍵)を生成します。

- 暗号化/認証
  IKEの暗号化に利用する暗号化アルゴリズムと認証に利用するハッシュアルゴリズムを設定します。
- 有効期間
  認証完了後の有効期間(秒)を設定します。1200〜28800秒まで設定することができます。

VPNパス(自動鍵交換:トンネルモード)画面

8. Phase1の「共有秘密鍵」を設定する。

IKEでの認証方法としてパスワードを利用するか、RSA鍵を利用するかを選択します。(VPNパスの概念図の⑤)

- パスワード(プリシェアードシークレット)
  事前に相手先と合意を取ったパスワード(プリシェアードシークレット)を用いて認証を行う場合は、「パスワード」を選択しテキストボックスにパスワードを入力します。
  パスワードは、接続先VPN機器と同じ接続パスワードとし、英数字を組み合わせて、8文字から500文字までで入力します。確認のため再入力してください。

VPNパス(自動鍵交換：トンネルモード)画面

- RSA鍵
  RSA鍵を利用する場合は、「RSA鍵」を選択しExpress5800/SG300が出力する鍵データと通信相手の機器が公開している鍵データの2つを設定します。

  ー 自ファイアウォールのRSA公開鍵を取得する
  「鍵の出力」をクリックしExpress5800/SG300のインストール時に作成した鍵をファイルに出力します。そのファイルを接続先VPN機器に渡して、RSA認証鍵として設定してください。

  ー 接続先VPN機器から取得した鍵を設定する
  接続先のVPN機器のRSA鍵を設定します。テキストボックスに、接続先VPN機器から出力した鍵ファイル名を指定します。ファイル名を直接入力するか、[参照]をクリックしてファイルを選択してください。
  鍵ファイル名を指定した後、[鍵IDの確認]をクリックすると、鍵IDの確認画面を別ウィンドウで表示します。

チェック

読み込む鍵ファイルは、ファイアウォールが動作している端末ではなく、Management Consoleを表示している管理クライアント上に保存してください。

ヒント

接続条件によっては、設定したアルゴリズムが使用されずIKEのネゴシエーションで自動選択されたアルゴリズムが使用されることがあります。

9. Phase2を設定する。

- 暗号化/認証
  AHを利用した認証を行う場合は、チェックボックスにチェックします。ハッシュアルゴリズムはMD5が適用されます。
  さらにESPで利用する暗号化アルゴリズムと認証アルゴリズム(ハッシュアルゴリズム)を設定します。

- 鍵の有効期間
  生成した鍵の有効期間(秒)を設定します。1200~86400秒まで設定することができます。

VPNパス(自動鍵交換：トンネルモード)画面

10. 必要なオプションのチェックボックスをチェックする。

- PFS(Perfect Forward Secrecy)の有効
  PFSを有効にします。PFSとは、万一、共有秘密鍵が解読された場合においても、VPN通信(IPSec)に利用する鍵(Phase2で生成)の解読ができないようにする方式です。

- IPSecで鍵更新を行う
  IPSecによるVPN通信で利用する鍵は、Phase2の項目で指定した有効期間を持ちます。「IPSecで鍵更新を行う」をチェックした場合、有効期間が切れた際に新たに鍵を生成して更新します。この機能により、鍵の有効期間を超えてVPN通信を継続することが可能になります。

- 適用時に有効化する
  「適用時に有効化する」をチェックした場合、設定の適用と同時にVPNの設定を行います。設定は行うもののVPN通信はまだ利用したくないというような場合は、「適用時に有効化する」をチェックせずに設定の適用を行ってください。

11. VPNパスに関する備考を入力する。

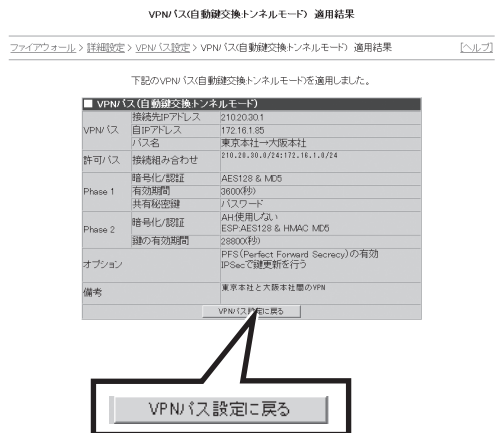
最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。入力は任意です。

12. [適用]をクリックする。

VPNパス(自動鍵交換：トンネルモード)適用結果画面が表示されます。

登録に失敗した場合には、エラー内容を示す画面を表示します。

13. [VPNパス設定に戻る]をクリックする。

追加したVPNパスが反映されたVPNパス設定画面が表示されます。

VPNパス(自動鍵交換:トンネルモード)適用結果画面

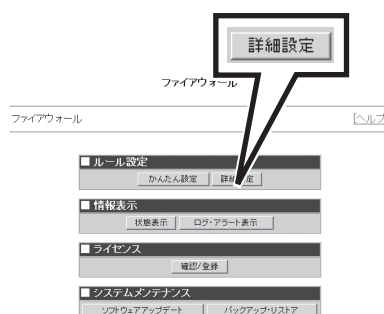
VPNパスの追加（自動鍵交換：トランスポートモード）

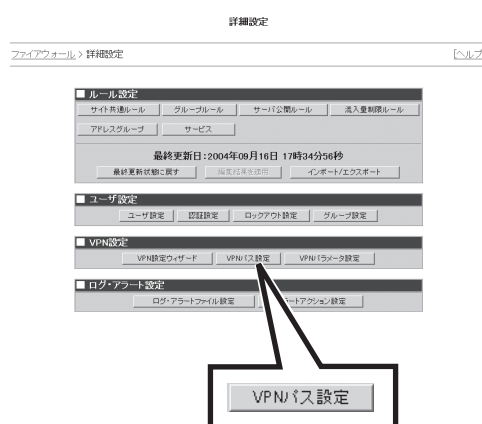
必要に応じてVPNパスを追加することができます。ここでは、トランスポートモードにおける自動鍵交換方式を利用したVPNパスの設定について説明します。VPN設定ウィザードでリモートアクセスVPNを設定した状態で新たなVPNパス（自動鍵交換：トランスポートモード）を追加するには、いったん設定済みのVPNパスを削除してから、以下の操作を行ってください。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

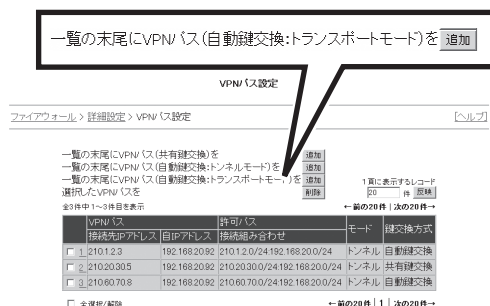
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

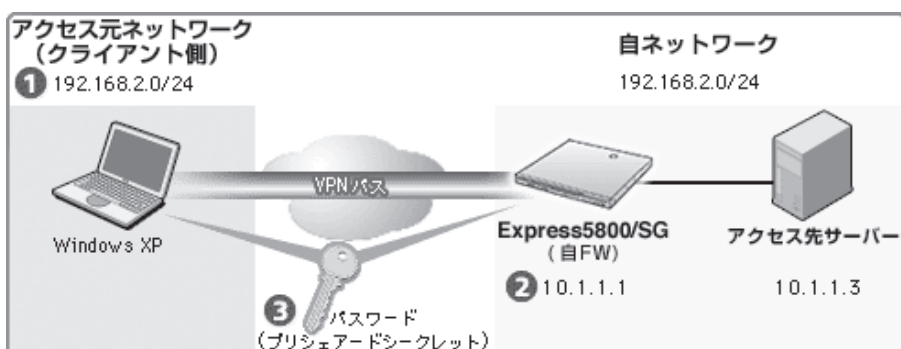
   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

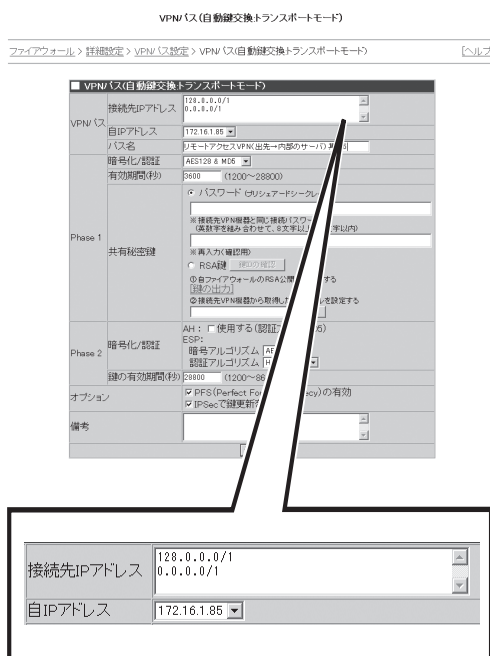
3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

   VPNパス設定画面が表示されます。

詳細設定メニュー画面

4. 「一覧の末尾にVPNパス(自動鍵交換：トランスポートモード)を『追加』」をクリックする。

VPNパス(自動鍵交換：トランスポートモード)画面が表示されます。

VPNパス設定画面

以降の各項目の設定手順では、VPN通信の概念を理解しやすくするために以下の図を用いて説明します。

5. VPNパスを設定する。

- 接続先アドレス
  VPNパスをはる接続先VPN機器が外部に公開しているIPアドレス、あるいはVPN機器が存在するネットワークアドレスを、一行に1つのアドレスの形式で入力します(VPNパスの概念図の①)。
- 自IPアドレス
  VPNパスをはる接続先から参照することができる、Express5800/SG300の外部ネットワークにつなげたインタフェースのIPアドレスをプルダウンメニューから選択します(VPNパスの概念図の②)。
- パス名
  VPNパスを識別する任意の文字列を指定します。VPNパス名は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

VPNパス(自動鍵交換：トランスポートモード)画面

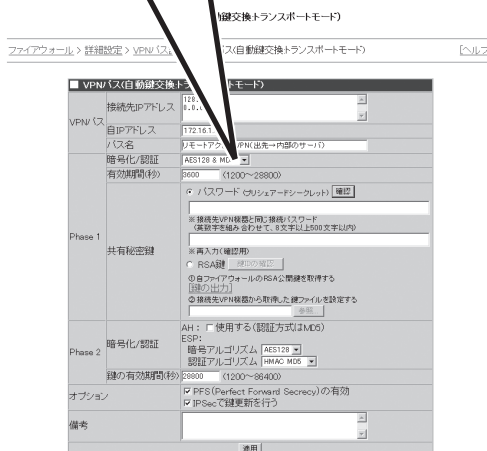
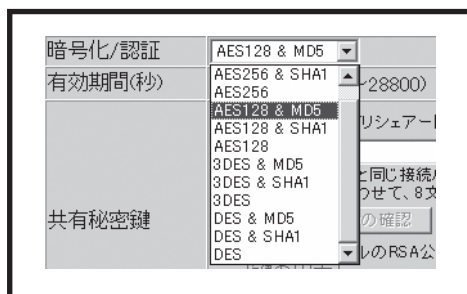
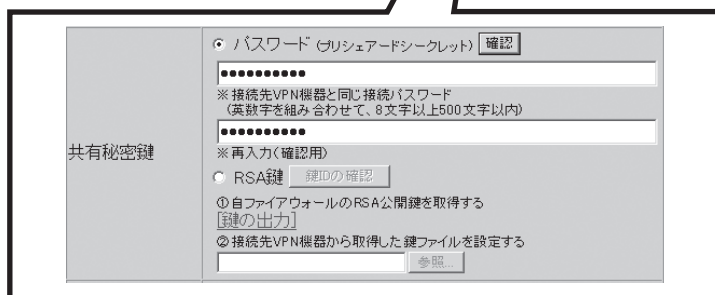
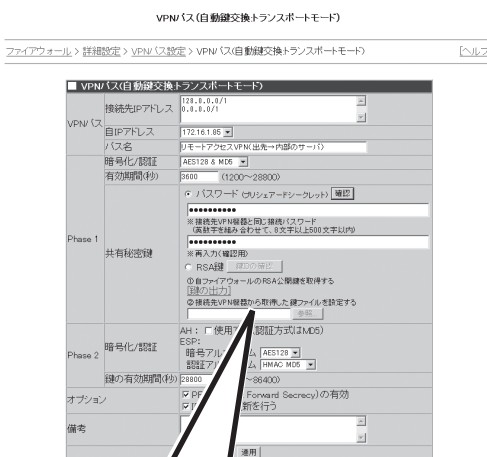
6. Phase1の「暗号化/認証」と「有効期間」を設定する。

VPNパス（自動鍵交換：トランスポートモード）画面

> **ヒント**
>
> 自動鍵交換方式では、最初にIKEを使って通信相手を認証し、暗号化アルゴリズムと暗号鍵を決定します。事前にパスワードまたはRSA鍵を共有していることが条件になります。
>
> IKEでは、まずハッシュアルゴリズムとパスワード（またはRSA鍵）を使って通信相手双方の認証を行います。認証完了後、暗号通信を利用して鍵の元となる乱数データと暗号化アルゴリズムを通知しあい、実際の通信で使用する共通鍵(秘密鍵)を生成します。

- 暗号化/認証
  IKEの暗号化に利用する暗号化アルゴリズムと認証に利用するハッシュアルゴリズムを設定します。
- 有効期間
  認証完了後の有効期間（秒）を設定します。1200〜28800秒まで設定することができます。

7. Phase1の「共有秘密鍵」を設定する。

IKEでの認証方法としてパスワードを利用するかRSA鍵を利用するかを選択します。（VPNパスの概念図の③）

VPNパス（自動鍵交換：トランスポートモード）画面

- パスワード(プリシェアードシークレット)
  事前に相手先と合意を取ったパスワード(プリシェアードシークレット)を用いて認証を行う場合は、「パスワード」を選択しテキストボックスにパスワードを入力します。
  パスワードには必ずアルファベットと数字の両方が含まれている必要があります。どちらか一方のみで構成されるパスワードは入力できません。確認のため再入力してください。

- RSA鍵
  RSA鍵を利用する場合は、「RSA鍵」を選択しExpress5800/SG300が出力する鍵データと通信相手の機器が公開している鍵データの2つを設定します。

  ー 自ファイアウォールのRSA公開鍵を取得する
  「鍵の出力」をクリックしExpress5800/SG300のインストール時に作成した鍵をファイルに出力します。そのファイルを接続先VPN機器に渡して、RSA認証鍵として設定してください。

  ー 接続先VPN機器から取得した鍵を設定する
  接続先のVPN機器のRSA鍵を設定します。テキストボックスに、接続先VPN機器から出力した鍵ファイル名を指定します。ファイル名を直接入力するか、[参照]をクリックして、ファイルを選択してください。
  鍵ファイル名を指定した後、[鍵IDの確認]をクリックすると、鍵IDの確認画面を別ウィンドウで表示します。

チェック

読み込む鍵ファイルは、ファイアウォールが動作している端末ではなく、Management Consoleを表示している管理クライアント上に保存してください。

ヒント

接続条件によっては、設定したアルゴリズムが使用されずIKEのネゴシエーションで自動選択されたアルゴリズムが使用されることがあります。

8. Phase2を設定する。

- 暗号化/認証
  AHを利用した認証を行う場合は、チェックボックスにチェックします。ハッシュアルゴリズムはMD5が適用されます。
  さらにESPで利用する暗号化アルゴリズムと認証アルゴリズム(ハッシュアルゴリズム)を設定します。

- 鍵の有効期間
  生成した鍵の有効期間(秒)を設定します。1200〜86400秒まで設定することができます。

VPNパス(自動鍵交換:トランスポートモード)画面

ファイアウォール機能の設定方法

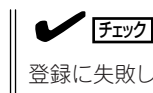
9. 必要なオプションのチェックボックスをチェックする。

- PFS(Perfect Forward Secrecy)
  PFSを有効にします。PFSとは、万一、共有秘密鍵が解読された場合においても、VPN通信(IPSec)に利用する鍵(Phase2で生成)の解読ができないようにする方式です。
- IPSecで鍵更新を行う
  IPSecによるVPN通信で利用する鍵は、Phase2の項目で指定した有効期間を持ちます。「IPSecで鍵更新を行う」をチェックした場合、有効期間が切れた際に新たに鍵を生成して更新します。この機能により、鍵の有効期間を超えてVPN通信を継続することが可能になります。

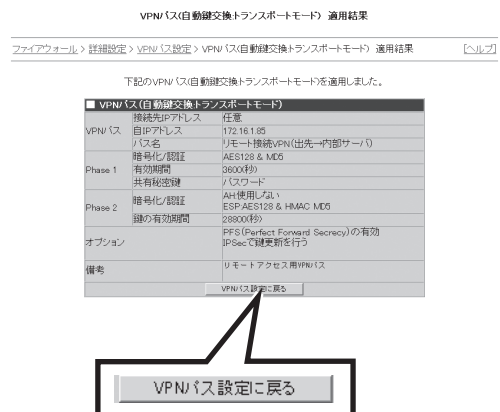
10. VPNパスに関する備考を入力する。

最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。入力は任意です。

11. [適用]をクリックする。

VPNパス(自動鍵交換：トランスポートモード)適用結果画面が表示されます。

登録に失敗した場合には、エラー内容を示す画面を表示します。

12. [VPNパス設定に戻る]をクリックする。

追加したVPNパスが反映されたVPNパス設定画面が表示されます。

VPNパス(自動鍵交換：トランスポートモード)適用結果画面

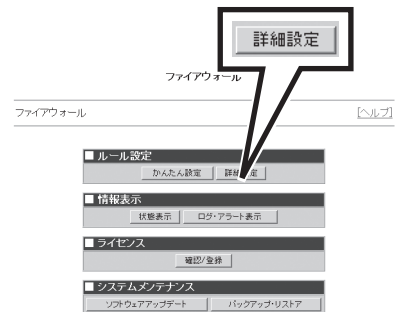
VPNパスの削除

不要になったVPNパスを削除することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

   VPNパス設定画面が表示されます。

詳細設定メニュー画面

4. 削除したいVPNパス番号の横に表示されるチェックボックスをチェックし、「選択したVPNパスを『削除』」をクリックする。

   VPNパス削除確認画面が表示されます。

   ヒント

   「全選択/解除」のチェックボックスをチェックすると、削除可能なVPNパスのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのVPNパスを削除対象から外すこともできます。

VPNパス設定画面

5. ［実行］をクリックする。

   - 背景が黄色で表示されたVPNパスは有効となっているVPNパスです。
   - 背景が赤色で表示されたVPNパスはグループルールで使用中です。まずグループルールの方からVPNパスを解除し、グループルールを適用してから、再度VPNパス削除を行う必要があります。
   - [中止]をクリックすると、削除されずにVPN情報一覧画面に戻ります。

   VPNパス削除結果画面が表示されます。

VPNパス削除確認画面

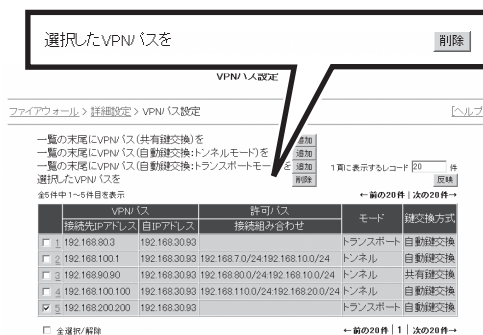
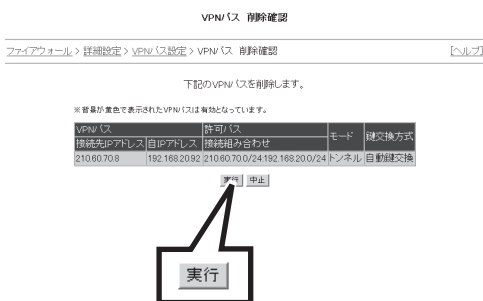
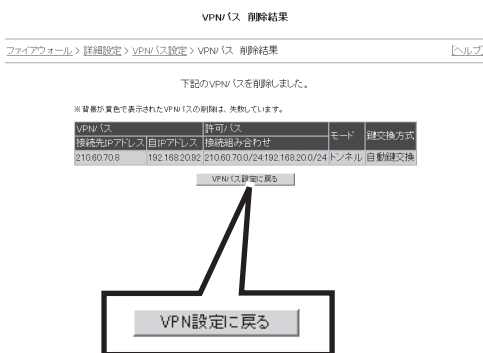
6. ［VPNパス設定に戻る］をクリックする。

   チェック

   背景が黄色で表示されたVPNパスは削除に失敗したVPNパスです。

   VPNパスが削除され、削除が反映したVPNパス設定画面が表示されます。

   重要

   現在有効なVPNパスを削除すると、そのVPNパスを使用して行っている通信も切断されます。

VPNパス削除結果画面

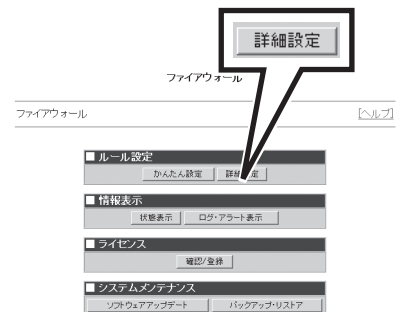
VPNパスの更新

一度設定したVPNパスの設定内容を変更することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

   VPNパス設定画面が表示されます。

詳細設定メニュー画面

4. 変更したいVPNパスの番号をクリックする。

   変更したいVPNパスのモード、鍵交換方式にしたがったVPNパス更新画面が表示されます。

VPNパス設定画面

5. 表示される各項目を設定する。

   それぞれの設定内容は追加設定と同様です。

6. ［適用］をクリックする。

   VPNパス適用結果画面が表示されます。

登録に失敗した場合には、エラー内容を示す画面を表示します。

VPNパス更新画面

7. ［VPNパス設定に戻る］をクリックする。

   変更したVPNパスが反映されたVPNパス設定画面が表示されます。

重要

現在有効なVPNパスを更新すると、そのVPNパスを使用して行っている通信も切断されることがあります。

下記のVPNパス(共有鍵交換)を適用しました。

■ VPNパス(共有鍵交換)		
VPNパス	接続先IPアドレス	210.20.30.5
	自IPアドレス	192.168.20.92
	パス名	特定ネットワーク→自ネットワーク
許可パス	接続組み合わせ	210.20.30.0/24:192.168.20.0/24
SPI値		780
■認証ヘッダ(AH)	ハッシュアルゴリズム	HMAC-MD5
	認証鍵	接続先VPN機器から取得した鍵
■暗号ペイロード(ESP)	暗号化アルゴリズム	AES
	共有鍵	自ファイアウォールの鍵
備考		

VPNパス設定に戻る

VPNパス設定に戻る

VPNパス適用結果画面

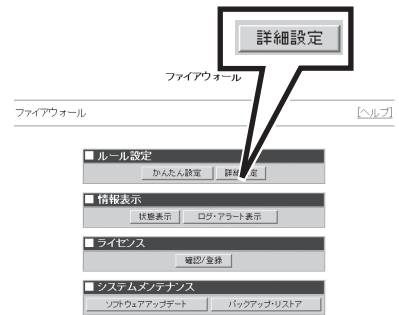
VPNパラメータの設定

Express5800/SG300で同時に利用できるVPNトンネル数、トランスポート数を設定することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパラメータ設定]をクリックする。

   VPNパラメータ設定画面が表示されます。

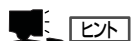
詳細設定メニュー画面

4. 利用できるVPNトンネルの数、トランスポートの数をそれぞれテキストボックスに入力する。

VPNパラメータ設定

ファイアウォール > 詳細設定 > VPNパラメータ設定 [ヘルプ]

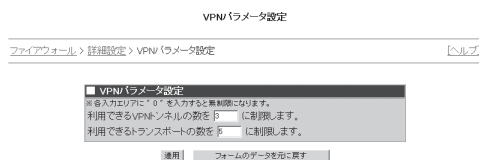
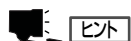
■ VPNパラメータ設定
※各入力エリアに"0"を入力すると無制限になります。
利用できるVPNトンネルの数を 3 に制限します。
利用できるトランスポートの数を 5 に制限します。

適用 フォームのデータを元に戻す

VPNパラメータ設定画面

ヒント

- **値は0～65535まで設定することができます。0を設定すると無制限になります。**
- **ユーザログインにより有効となったトランスポートモードのセッションは、セッションの有効期間終了後、鍵の有効期間が切れるまでが、トランスポート数の計算対象となります。**

5. ［適用］をクリックする。

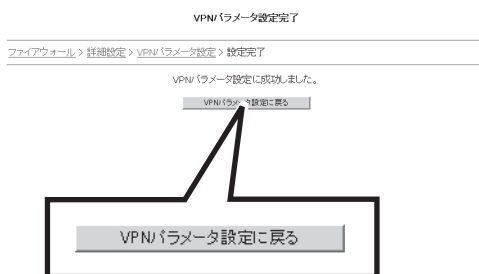
ヒント

[フォームのデータを元に戻す]をクリックすると、前回設定した値に戻ります。

VPNパラメータ設定完了画面が表示されます。

重要

[適用]をクリックするとVPNの接続が一時切断されます。

6. ［VPNパラメータ設定に戻る］をクリックする。

VPNパラメータ設定画面が表示されます。

VPNパラメータ設定完了画面

ログ・アラート設定

Express5800/SG300が出力するログファイル、アラートファイルに関連する各種パラメータを設定することができます。
ログ・アラート設定では以下の項目を設定することができます。

ログ・アラートファイル設定 .... Express5800/SG300が出力するログファイル、アラートファイルのパラメータを設定します。

ログ・アラートファイルダウンロード/アップロード.......... ログ・アラートファイルを管理クライアントにダウンロードしたり、ダウンロードしたファイルをExpress5800/SG300にアップロードします。

アラートアクション設定 .... アラート発生時のアクションを設定します。

ログ・アラートファイル設定

Express5800/SG300が出力するログファイル、アラートファイルの収集時間や出力内容などの各種パラメータを設定することができます。

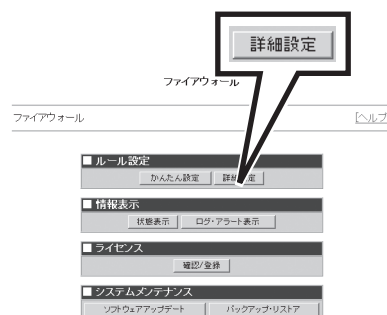
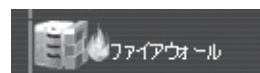
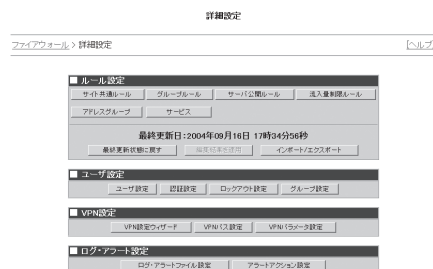
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

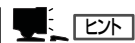
3. 詳細設定メニューの「ログ・アラート設定」から[ログ・アラートファイル設定]をクリックする。

   ログ・アラートファイル設定画面が表示されます。

詳細設定メニュー画面

4. ログ・アラートファイル設定画面に表示される各項目を設定する。

ログ・アラートファイル設定画面

設定	ローテーションサイズ	1つのファイルの最大サイズを4096KB(4MB)から65536KB(64MB)の範囲で指定します。 通常ログファイルは1日単位でローテーションを行いますが、ログファイルサイズが指定サイズを超えた場合には、1日単位のローテーションとは別にローテーションを行います。
	ログ保存期間	ファイルを残す日数を指定します。1日から2000日までの範囲で指定します。 なお、ログを保存しているパーティションの残量が少なくなった場合には、下記の残量確保の設定により、古いログファイルから削除されます。 この場合、指定した保存期間に達する前に削除されます。
	パーティション残量確保	ログを出力するシステムのパーティションに確保する空き容量を指定します。パーティション容量が指定値以下になると、古いログから順に指定残量が確保できるまで削除します。 32768KB(32MB)から1048576KB(1GB)までの範囲で指定します。
	ログ参照	チェックすると、ログを参照したときに参照情報をログとして記録します。

5. ［適用］をクリックする。

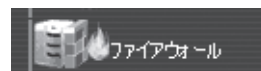
ヒント

[フォームのデータを元に戻す]をクリックすると、適用前の設定値に戻ります。

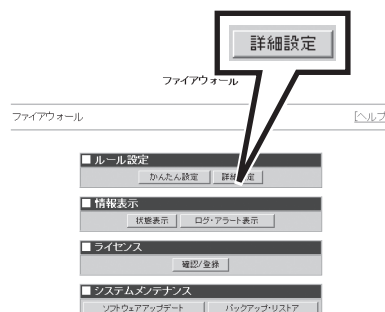
6. 別ウィンドウで更新確認ダイアログメッセージが表示されるので、［OK］をクリックする。

ログ・アラートファイルダウンロード／アップロード

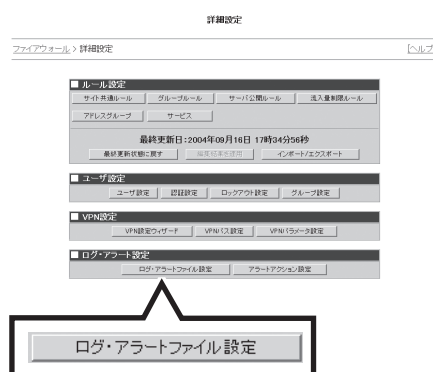
ログ・アラートファイルを管理クライアントにダウンロードしたり、ダウンロードしたファイルをExpress5800/SG300にアップロードすることができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ログ・アラート設定」から[ログ・アラートファイル設定]をクリックする。

   ログ・アラートファイル設定画面が表示されます。

詳細設定メニュー画面

4. ログ・アラートファイルダウンロード／アップロードメニューから実行する操作を選択する。

ログ・アラートファイル設定画面

ダウンロード/アップロード	ダウンロード	日付指定でログ・アラートファイルをコンソール端末上にダウンロードします。
	アップロード	ログファイルを指定してExpress5800/SG300にアップロードします。アップロードされたファイルはログ保存期間を過ぎても残されます。またパーティション残量確保時でも削除対象となりません。なお、アップロードにより保存されるファイルは1ファイルのみです。新しいファイルをアップロードすると保存されているファイルは削除されます。アップロードしたファイルは「ログ・アラート表示」から確認できます。「ログ・アラート表示」については、289ページを参照してください。
	アップロードファイルの削除	アップロードされているファイルを削除します。

5. [実行]をクリックする。

指定した操作が実行されます。

●ダウンロード

ファイルのダウンロード画面が表示されるので[保存]をクリックして、保存場所を指定します。

●アップロード

[参照]をクリックしてファイルを指定してから[実行]をクリックします。確認画面が表示されるので[OK]をクリックします。

●アップロードファイルの削除

別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックします。別ウィンドウで完了確認のダイアログメッセージが表示されるので[OK]をクリックします。

ログ・アラートファイル設定画面

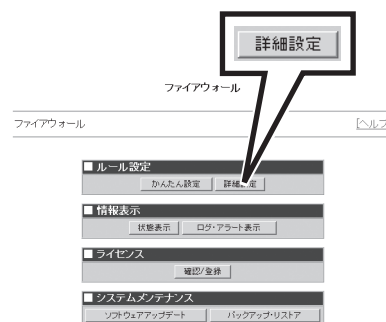
アラートアクション設定

アラート出力時に行うアクションの設定を行います。

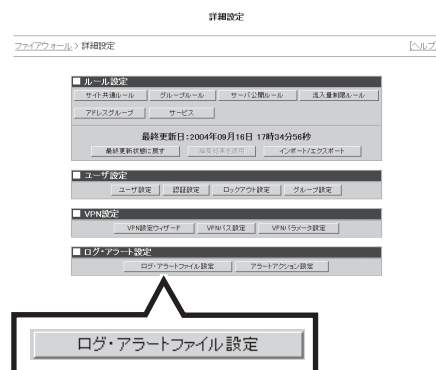
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

ファイアウォールメニュー画面

3. 詳細設定メニューの「ログ・アラート設定」から[アラートアクション設定]をクリックする。

   アラートアクション設定画面が表示されます。

詳細設定メニュー画面

4. アラートアクション設定画面に表示される各項目を設定する。

項　目		説　明
通知方法	メール送付	アラート発生をメールにて通知します。通知するメールアドレスを3つまで登録できます。「送信元アドレス」には、メールの送信元を指定できます。
	SYSLOG出力	アラート発生をSYSLOGで出力します。出力するファシリティとレベルを設定します。
	コマンド実行	アラート発生時にコマンドを実行します。実行するコマンドを登録します。
通知間隔		通知間隔を60秒から86400秒までの範囲で指定します。
メッセージ	同一出力の抑制	チェックすると、同様のアラートが「通知間隔」で指定した間に発生した時に、アクションの実行を抑制するとともに、メール通知、もしくはsyslogの出力で同様のアラートが連続した回数のみ出力されても、最初のアラートを一度だけ出力するようになります。
	アドバイザリの出力（メールのみ）	チェックすると、アラートについての対処方法を含んだメッセージを送ります。ただし、この機能は、「メール送付」による通知でのみ有効です。
通知イベント		イベントごとに行うアクションのチェックボックスをチェックすることで設定します。メール1はメール送付の「アドレス1」、メール2は「アドレス2」にメールを送信することを意味しています。

アラートアクション設定

ファイアウォール > 詳細設定 > アラートアクション設定　[ヘルプ]

■ アラートアクション設定

通知方法	メール送付	アドレス1: / アドレス2: / アドレス3: / 送信元アドレス: <Alerter@localhost>
	SYSLOG出力	ファシリティ: LOCAL5　レベル: ALERT
	コマンド実行	
通知間隔	120 秒	
メッセージ	□同一出力の抑制 □アドバイザリの出力(メールのみ)	

通知イベント	イベント種別	メール1	メール2	メール3	SYSLOG	コマンド	自動防御
	SYN-SCAN検出	□	□	□	□	□	□
	SYN-FLOOD検出	□	□	□	□	□	
	PING-SWEEP検出	□	□	□	□	□	□
	パケット受付	□	□	□	□	□	
	パケット拒否	□	□	□	□	□	
	通信ログ(上記以外)	□	□	□	□	□	
	ウェブ/メールフィルタ	□	□	□	□	□	
	ユーザ認証	□	□	□	□	□	
	ファイル改ざん監視	□	□	□	□	□	
	プロセス監視	□	□	□	□	□	
	その他(上記以外)	□	□	□	□	□	

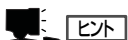
更新　フォームのデータを元に戻す

アラートアクション設定画面

ヒント

[通知イベント]にある[自動防御]は、[SYN-SCAN検出]と[PING-SWEEP検出]イベントについて選択できるオプションです。このオプションを有効にすると、[SYN-SCAN検出]、または[PING-SWEEP検出]イベントを検出した際、Express5800/SG300は自動的に送信元との通信を一時的に遮断します。

5. [更新]をクリックする。

ヒント

- [フォームのデータを元に戻す]をクリックすると、適用前の設定値に戻ります。
- メールアドレス部分には、必ず有効なメールアドレスを指定してください。
  メールの送信時にはアドレスのチェックは行わないため、不正なアドレスが指定された場合、メールはそのまま送信され、エラーになる場合があります。

6. 更新結果ダイアログメッセージが表示されるので[OK]をクリックする。

   アラートアクションが設定されます。

情報表示

Express5800/SG300の情報を表示することができます。
情報表示では以下の項目を表示することができます。

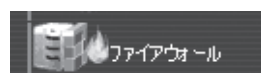
状態表示 .... Express5800/SG300の状態を表示することができます。

ログ・アラートの表示 .... Express5800/SG300の出力するログおよびアラート情報を表示することができます。

状態表示

Express5800/SG300が正常に起動中であるか、あるいは異常状態であるかを表示することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「情報表示」から[状態表示]をクリックする。

   状態表示画面が表示されます。以下のような状態が表示されます。

ファイアウォールメニュー画面

状態表示画面

- 現在、正常動作中
  Experess5800/SG300はファイアウォール装置として正常に稼動中です。
- 現在、停止中
  ファイアウォールは停止しています。
- 現在、障害発生中
  何らかの原因によりファイアウォールに障害が発生しており、一部機能が停止しています。
  次ページの「ログ・アラート表示」を参照してエラーが出ていないか確認してください。
  なお、状態の右側に表示される以下のボタンをクリックすることで、Experess5800/SG300を起動、再起動、停止することができます。
- 現在、現用中
  二重化構成時、運用系の機器として正常に稼働中です。
- 現在、待機中
  二重化構成時、待機系の機器としてホットスタンバイしています。

- 停止する
  Experess5800/SG300が停止中以外の場合にクリックすると停止します。
- 再起動する
  クリックするとExperess5800/SG300を再起動します。
- 起動する
  Experess5800/SG300の停止時にクリックすると起動します。

ログ・アラート表示

Express5800/SG300が出力するログ情報およびアラート情報を表示/出力することができます。以下のような表示/出力をすることができます。

- ログ表示
- CSV出力
- 簡易集計表示
- 外部統計用CSV出力

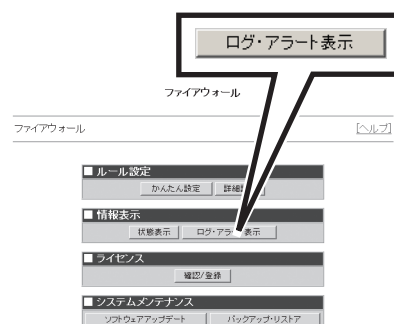
ログ表示

Express5800/SG300が出力するログ情報およびアラート情報を表示することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

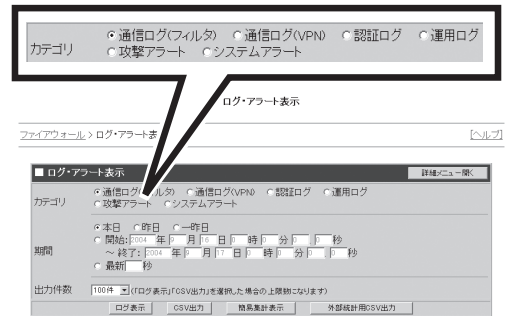
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。

   ログ・アラート表示画面が表示されます。

ファイアウォールメニュー画面

3. 表示するログのカテゴリを選択する。

ログ・アラート表示画面

- 通信ログ(フィルタ)
  フィルタリング機能によるパケットの通過、拒否、破棄のログを表示します。表示される通信は、サイト共通ルール、グループルールで、ログを記録すると設定したもののみです。
- 通信ログ(VPN)
  VPNパスを利用した通信のログを表示します。
- 認証ログ
  ユーザ認証のログを表示します。
- 運用ログ
  Express5800/SG300の起動や停止など運用情報のログを表示します。
- 攻撃アラート
  Express5800/SG300が攻撃を検出したときに出力するアラート情報です。
- システムアラート
  Express5800/SG300の運用上のアラート情報です。

4. 期間を選択する。

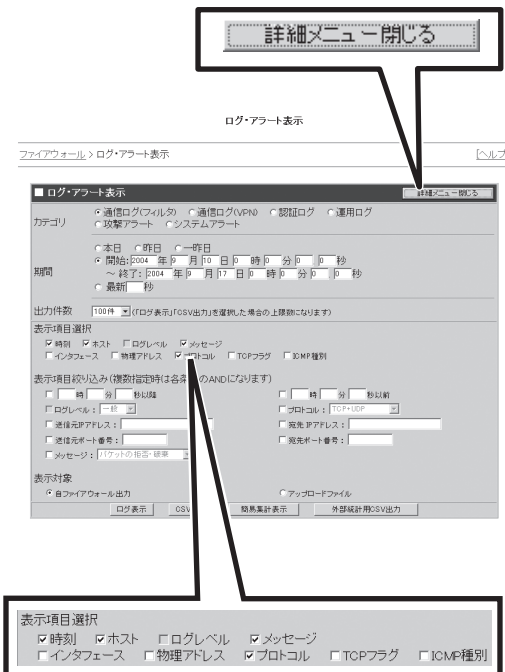
   「本日」、「昨日」、「一昨日」をクリックするとそれぞれ指定した一日分のログを表示します。
   それ以外の日や数日に渡ってログを取得する場合は、「開始」のラジオボタンを選択し、開始から終了までの年月日時分秒を指定します。
   「最新」をクリックしてテキストボックスに秒を設定すると、指定した直近の秒までのログを表示します。

5. 表示するログの上限となる「出力件数」をプルダウンメニューから選択する。

6. さらに詳しく条件を設定する場合はタイトルバーの右側にある[詳細メニュー開く]をクリックする。

   詳細メニューが表示されます。

   ヒント

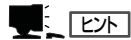
   - 特に詳細条件を指定しない場合は手順8に進みます。
   - [詳細メニュー閉じる]をクリックすると詳細メニューが閉じます。

ログ・アラート表示(詳細メニュー)画面

7. ログの表示条件の詳細な設定を行う。

カテゴリ	項　目		説　明
通信ログ （フィルタ）	表示項目 選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
		インタ フェース	チェックすると通信のインタフェースが表示されます。
		物理アドレス	チェックするとインタフェースの物理アドレスが表示されます。
		プロトコル	チェックすると通信種別が表示されます。
		TCPフラグ	TCP通信の場合、チェックするとフラグの状態が表示されます。
		ICMP種別	ICMP通信の場合、チェックすると通信種別が表示されます。
	表示項目 絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
		プロトコル	表示するプロトコルをプルダウンメニューから選択します。
		送信元IP アドレス	表示する送信元IPアドレスを指定します。
		送信元 ポート番号	表示する送信元ポート番号をプルダウンメニューから選択します。
		宛先IP アドレス	表示する宛先IPアドレスを指定します。
		宛先 ポート番号	表示する宛先ポート番号を指定します。
		メッセージ	チェックしてメッセージの種類を選択します。
通信ログ （VPN通信） 運用ログ 認証ログ	表示項目 選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		ログレベル	チェックするとログレベルが表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目 絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
		ログレベル	表示するログレベルをプルダウンメニューから指定します。
攻撃 アラート	表示項目 選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目 絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
システム アラート	表示項目 選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目 絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
すべて	表示対象	自ファイア ウォール出力	自ファイアウォール（Express5800/SG300）が出力したファイルを表示します。
		アップロード ファイル	Express5800/SG300にアップロードしたファイルを表示します。

8. ［ログ表示］をクリックする。

指定した条件のログ情報が別ウィンドウで表示されます。

ヒント

- 「キーワードサーチ」のテキストボックスにキーワードを入力し[検索]をクリックすると、検索した条件のログのみを表示します。検索した条件に当てはまらないログは一覧に表示されません。また、2つ以上の条件検索はすることができません。
- 表中のヘッダ（背景緑色の部分）をクリックすると、その列でソートすることができます。
- キーワードサーチやソートの対象となるのは、そのとき画面に表示されているもののみです。

期間の指定で「最新」を選択した場合は、オートリフレッシュ機能が利用できます。「オートリフレッシュ」のチェックボックスにチェックすると、5秒ごとに自動的にログを再取得し、表示を更新します。ただし、この場合は、キーワードサーチとソートを行うことはできません。

9. ［このウィンドウを閉じる］をクリックする。

ログ情報表示画面が閉じます。

時刻	ホスト	メッセージ	発信元IPアドレス	発信元ポート番号	宛先IPアドレス	宛先ポート番号	プロトコル
2004/09/10 11:28:20.315	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:20.465	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:20.515	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:20.935	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:21.775	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:23.455	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:23.665	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:26.815	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:33.535	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:28:46.975	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:29:13.855	b092.fwt.isd.nec.co.jp	不明な接続を検出しました	192.168.9.89	57526	192.168.9.92	18022	TCP
2004/09/10 11:47:30.955	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.161	33268	192.168.30.92	443	TCP
2004/09/10 11:50:08.635	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.161	33270	192.168.30.92	443	TCP
2004/09/10 11:50:11.635	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.161	33270	192.168.30.92	443	TCP
2004/09/10 11:50:17.635	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.161	33270	192.168.30.92	443	TCP
2004/09/10 11:50:41.235	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.161	33271	192.168.30.92	443	TCP
2004/09/10 12:00:30.995	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.92	1265	192.168.30.92	139	TCP
2004/09/10 12:00:31.015	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.92	1180	192.168.30.92	139	TCP
2004/09/10 12:00:31.035	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.92	1499	192.168.30.92	139	TCP
2004/09/10 12:00:31.055	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.92	1687	192.168.30.92	139	TCP
2004/09/10 12:00:31.075	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.92	2247	192.168.30.92	139	TCP
2004/09/10 12:00:31.095	b092.fwt.isd.nec.co.jp	SPOOFING を検出しました	192.168.30.92	2185	192.168.30.92	139	TCP

ログ情報表示画面

CSV出力

Express5800/SG300が出力するログ情報をCSVファイルに出力することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから［ファイアウォール］をクリックする。

ファイアウォールメニュー画面が表示されます。

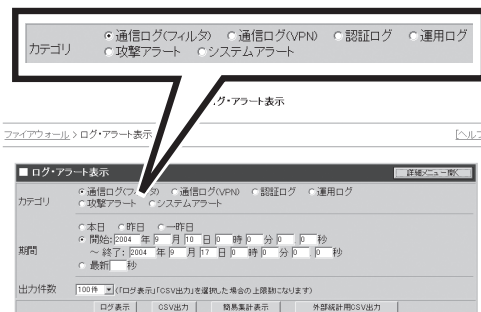
2. ファイアウォールメニューの「情報表示」から［ログ・アラート表示］をクリックする。

ログ・アラート表示画面が表示されます。

ファイアウォールメニュー画面

3. CSVファイルに出力するログのカテゴリを選択する。

ログ・アラート表示画面

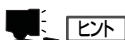
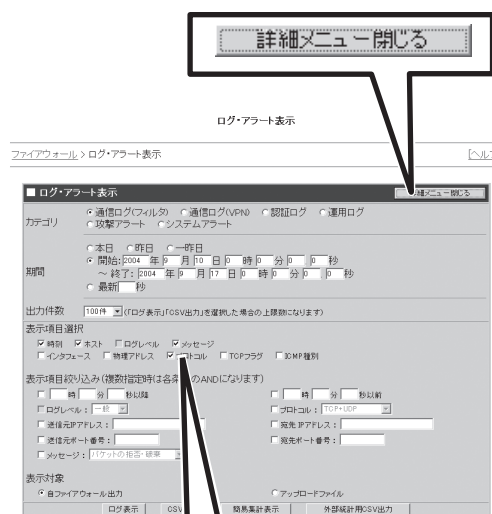
- 通信ログ(フィルタ)
  フィルタリング機能によるパケットの通過、拒否、破棄のログをCSVファイルに出力します。CSVファイルに出力される通信は、サイト共通ルール、グループルールで、ログを記録すると設定したもののみです。
- 通信ログ(VPN)
  VPNパスを利用した通信のログをCSVファイルに出力します。
- 認証ログ
  ユーザ認証のログをCSVファイルに出力します。
- 運用ログ
  Experess5800/SG300の起動や停止など運用情報のログをCSVファイルに出力します。
- 攻撃アラート
  Express5800/SG300が攻撃を検出したときに出力するアラート情報です。
- システムアラート
  Express5800/SG300の運用上のアラート情報です。

4. 期間を選択する。

「本日」、「昨日」、「一昨日」をクリックするとそれぞれ指定した一日分のログをCSVファイルに出力します。
それ以外の日や数日に渡ってログを出力する場合は、「開始」のラジオボタンを選択し、開始から終了までの年月日時分秒を指定します。
「最新」をクリックしてテキストボックスに秒を設定すると、指定した直近の秒までのログを出力します。

5. 出力するログの上限となる「出力件数」をプルダウンメニューから選択する。

6. さらに詳しく条件を設定する場合はタイトルバーの右側にある[詳細メニュー開く]をクリックする。

詳細メニューが表示されます。

ヒント

- 特に詳細条件を指定しない場合は手順8に進みます。
- [詳細メニュー閉じる]をクリックすると詳細メニューが閉じます。

ログ・アラート表示(詳細メニュー)画面

7. ログの出力条件の詳細な設定を行う。

カテゴリ	項　目		説　明
通信ログ（フィルタ）	表示項目選択	時刻	チェックすると時刻が出力されます。
		ホスト	チェックするとホスト名が出力されます。
		メッセージ	チェックするとメッセージが出力されます。
		インタフェース	チェックすると通信のインタフェースが出力されます。
		物理アドレス	チェックするとインタフェースの物理アドレスが出力されます。
		プロトコル	チェックすると通信種別が出力されます。
		TCPフラグ	TCP通信の場合、チェックするとフラグの状態が出力されます。
		ICMP種別	ICMP通信の場合、チェックすると通信種別が出力されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
		プロトコル	表示するプロトコルをプルダウンメニューから選択します。
		送信元IPアドレス	表示する送信元IPアドレスを指定します。
		送信元ポート番号	表示する送信元ポート番号を指定します。
		宛先IPアドレス	宛先IPアドレスを指定します。
		宛先ポート番号	宛先ポート番号を指定します。
		メッセージ	チェックしてメッセージの種類を選択します。
運用ログ 認証ログ 通信ログ（VPN通信）	表示項目選択	時刻	チェックすると時刻が出力されます。
		ホスト	チェックするとホスト名が出力されます。
		ログレベル	チェックするとログレベルが出力されます。
		メッセージ	チェックするとメッセージが出力されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
		ログレベル	表示するログレベルをプルダウンメニューから指定します。
攻撃アラート	表示項目選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
システムアラート	表示項目選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
すべて	表示対象	自ファイアウォール出力	自ファイアウォール(Express5800/SG300)が出力したファイルをCSV出力します。
		アップロードファイル	Express5800/SG300にアップロードしたファイルをCSV出力します。

8. ［CSV出力］をクリックする。

CSVファイルの保存画面が表示されるので保存先を決定します。

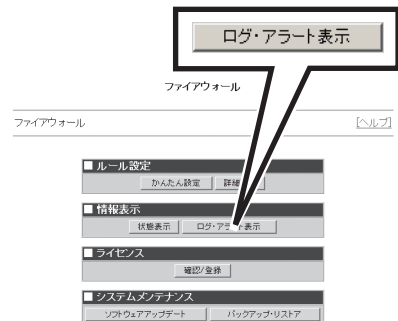
簡易集計表示

Express5800/SG300が保存している通信ログ情報を簡易集計し、グラフィカルに表示することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

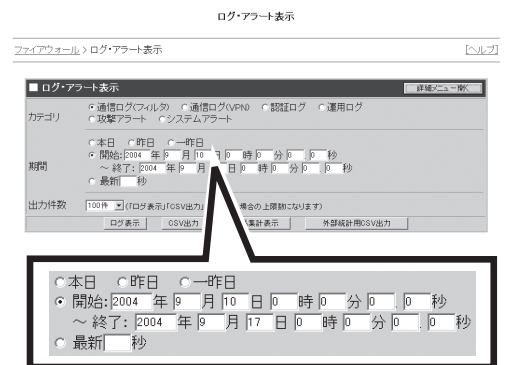
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。

   ログ・アラート表示画面が表示されます。

ファイアウォールメニュー画面

3. 期間を選択する。

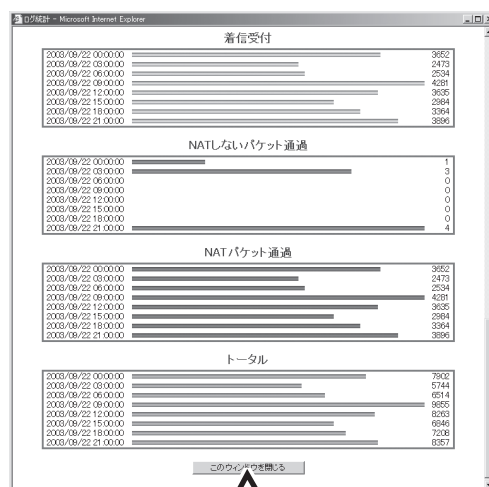
   「本日」、「昨日」、「一昨日」をクリックするとそれぞれ指定した一日分のログを表示します。
   それ以外の日や数日に渡ってログを取得する場合は、「開始」のラジオボタンを選択し、開始から終了までの年月日時分秒を指定します。
   「最新」をクリックしてテキストボックスに秒を設定すると、指定した直近の秒までのログを表示します。

   簡易集計表示では、「期間」以外の項目は指定できません。

ログ・アラート表示画面

4. [簡易集計表示]をクリックする。

   指定した日付のログ情報の簡易集計が別ウィンドウで表示されます。

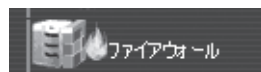
5. [このウィンドウを閉じる]をクリックする。

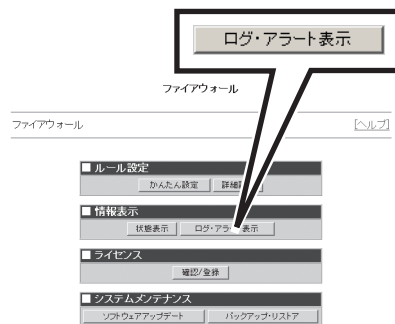
簡易集計表示画面が閉じます。

簡易集計表示画面

外部統計用CSV出力

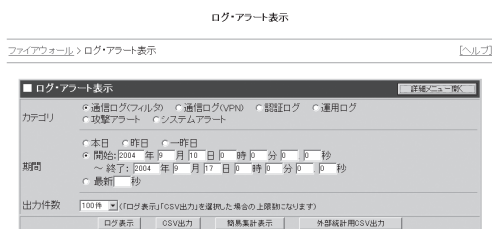
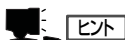
外部集計ツールで利用するCSVファイルを出力することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。

   ログ・アラート表示画面が表示されます。

ファイアウォールメニュー画面

3. 期間を選択する。

   「本日」、「昨日」、「一昨日」をクリックするとそれぞれ指定した一日分のログをCSVファイルに出力します。
   それ以外の日や数日に渡ってログを出力する場合は、「開始」のラジオボタンを選択し、開始から終了までの年月日時分秒を指定します。
   「最新」をクリックしてテキストボックスに秒を設定すると、指定した直近の秒までのログを出力します。

ログ・アラート表示画面

> **ヒント**
> 外部統計用CSV出力では、「期間」以外の項目は指定できません。

4. [外部統計用CSV出力]をクリックする。

   CSVファイルの保存画面が表示されるので保存先を決定します。

ライセンスの確認と登録

Express5800/SG300を利用するには、ライセンスキーの登録を行う必要があります。またサポートキーを登録すると、ソフトウェアおよびOSのサポートサービスを受けることができます。ライセンスキー、サポートキーの取得については、1章の「ライセンスキー」および「ソフトウェアサポートサービス」を参照してください。

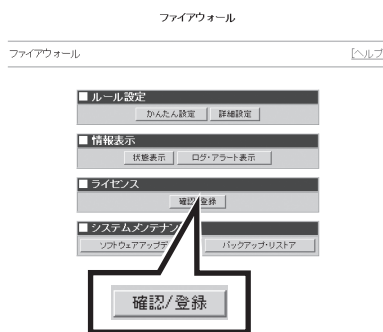
ライセンスキー／サポートキーの登録

Express5800/SG300では、ファイアウォールとして動作させるために必要なライセンスキーと、サポートサービスを受けるために必要なサポートキーの2種類のキーによりライセンスを管理しています。
Express5800/SG300を利用するには、はじめにライセンスの登録を行う必要があります。

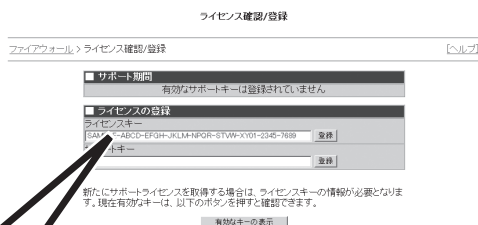
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

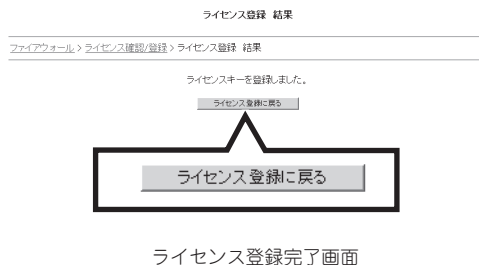
   ファイアウォールメニュー画面が表示されます。

2. 「ファイアウォール」メニューの「ライセンス」から[確認/登録]をクリックする。

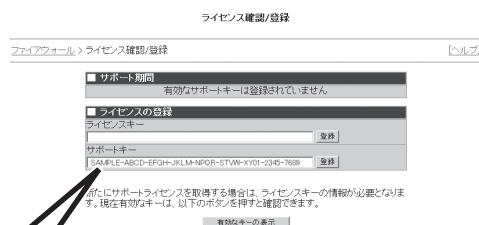
   ライセンスの確認と登録画面が表示されます。

ファイアウォールメニュー画面

3. 「ライセンスキー」のテキストボックスに購入先より通知されたライセンスキーを入力し、[登録]をクリックする。

   ライセンスの登録完了画面が表示されます。

ライセンス確認/登録画面

4. ［ライセンス登録に戻る］をクリックする。

ライセンス登録完了画面

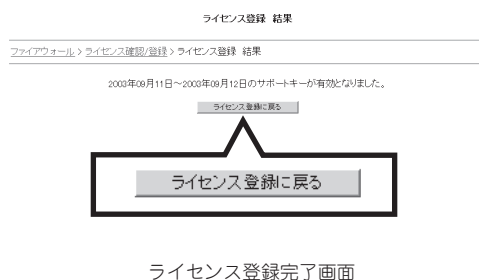
5. ソフトウェアサポートサービスを購入している場合は、「サポートキー」のテキストボックスに購入先より通知されたサポートキーを入力し、［登録］をクリックする。

ライセンスの登録完了画面が表示されます。

ライセンス確認/登録画面

6. ライセンスの有効期限を確認し［ライセンス確認/登録に戻る］をクリックする。

重要

サポートキーはライセンスキーを登録していないと登録できません。

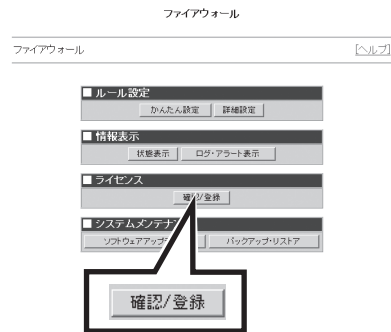
ライセンス登録完了画面

ライセンス設定の確認

登録したライセンスキー/サポートキーを確認することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

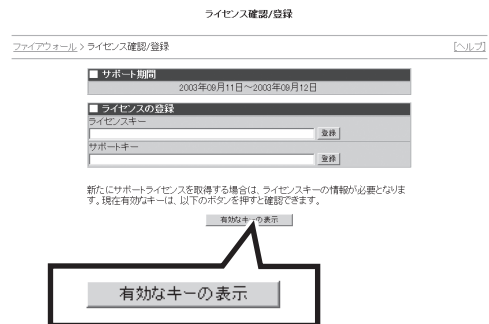
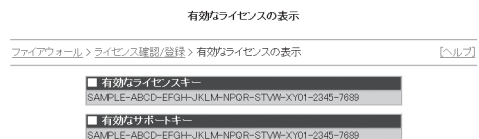
   「ファイアウォール」メニュー画面が表示されます。

2. 「ファイアウォール」メニューでライセンスの[確認/登録]をクリックする。

   ライセンスの確認と登録画面が表示されます。

ファイアウォールメニュー画面

3. [有効なキーの表示]をクリックする。

   ライセンスの確認画面が表示され、有効なライセンスキー、およびサポートキーが確認できます。

登録済みのライセンスキーであっても有効期限切れや無効のキーは表示されません。

ライセンス確認/登録画面

有効なライセンス表示画面

システムメンテナンス

管理者は、Express5800/SG300のソフトウェアのアップデートや、設定したルール、グループ情報などのデータのバックアップ/リストアをすることができます。

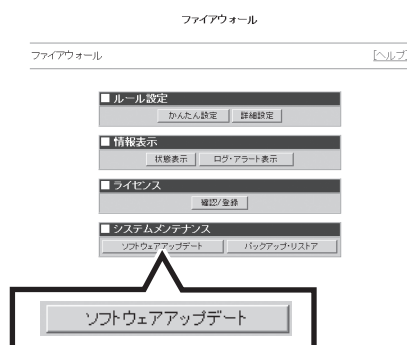
ソフトウェアアップデート

ソフトウェアサポートサービスを購入している場合は、インターネットを利用してソフトウェアおよびOSを利用可能な最新状態へアップデートすることができます。

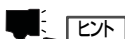
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

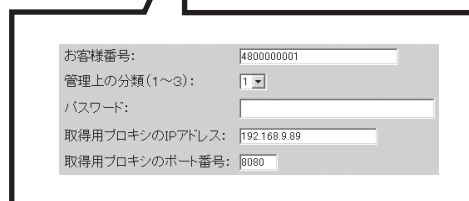
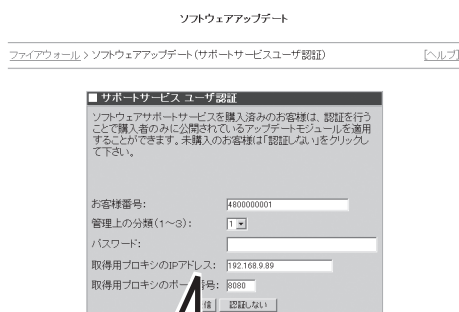
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「システムメンテナンス」から[ソフトウェアアップデート]をクリックする。

   サポートサービスユーザ認証画面が表示されます。

ファイアウォールメニュー画面

3. 画面に従い以下の項目を入力する。

   - お客様番号
   - 管理上の分類
   - パスワード

   ヒント

   お客様番号、管理上の分類番号、パスワードは製品購入時に通知されたものを入力します。お客様番号はライセンス登録を行っていれば自動的に表示されます。

サポートサービスユーザ認証画面

4. 外部ネットワークへ通信するためにプロキシを利用している場合は、以下の項目についても入力する。

- 取得用プロキシのIPアドレス
- 取得用プロキシのポート番号

ヒント

プロキシを利用していない場合は空欄のままにしておきます。

重要

サポートサービスユーザ認証画面を表示しているブラウザも、アップデートパッケージの情報を取得するためにサポートサービスサイトに直接アクセスを行います。そのため、事前に管理クライアントからの外部ネットワークへのHTTP通信を許可しておく必要があります。フィルタリングの設定については135ページの「内部から外部への通信におけるウェブ専用フィルタの設定」を参照してください。

また、インターネットへ通信するためにHTTPプロキシの設定が必要な場合は、ブラウザ自身にプロキシの設定を行ってください。

5. [送信]をクリックする。

ユーザ認証が行われます。

ヒント

ユーザ認証に失敗した場合には、ユーザ認証画面に戻ります。

ユーザ認証に成功すると、Express5800/SG300はあらかじめ定められたサイトと通信し、アップデート情報の取得をします。

配布可能なアップデート情報の一覧を示したアップデート画面が表示されます。

アップデート解析画面

チェック

[認証しない]をクリックした場合は、Express5800/SG300はあらかじめ定められたサイトと通信し、認証を経ていないユーザにも配布可能なアップデート情報を取得し、アップデート情報の一覧を示したアップデート画面を表示します。

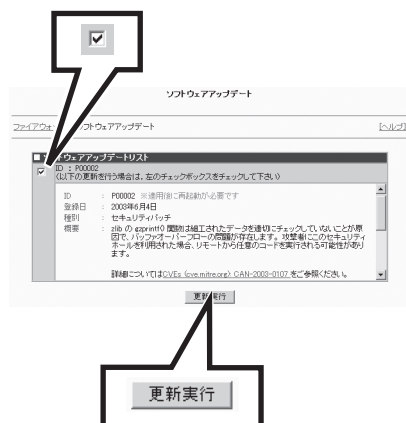
ヒント

- サイトとの通信に失敗した場合は、エラー画面が表示されます。フィルタリング設定、プロキシの設定を確認してください。
- アップデートの必要がない場合は、「アップデート対象のソフトウェアはありません」画面が表示されます。[戻る]をクリックしてください。

6. アップデート画面において、適用したいアップデート情報のチェックボックスをチェックし、[更新実行]をクリックする。

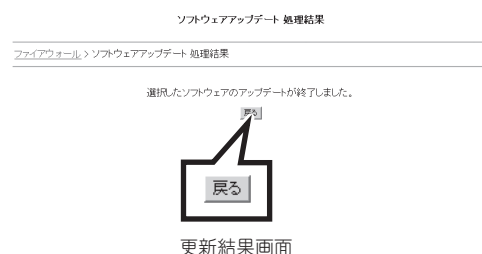
選択したアップデート情報をExpress5800/SG300に適用します。

重要

アップデート情報の内容によっては、適用後すぐにシステムの再起動を必要とするものがあります。適用後すぐにシステムの再起動が必要な場合は[更新実行]をクリックすると、再起動実行の確認画面が表示されます。再起動しても問題がなければ[OK]をクリックしてください。

アップデート画面

アップデート情報の適用に成功すると更新結果画面が表示されます。

7. [戻る]をクリックする。

ファイアウォールメニュー画面に戻ります。

更新結果画面

ヒント

適用後すぐにシステムの再起動が必要な更新の場合は、更新結果画面(システム再起動時)が表示され、システムの再起動が自動的に行われます。再起動したら再度Management Consoleにログインしてください。

なお、適用後すぐにシステムの再起動を必要とするアップデートは一度に1つのパッケージしか適用できません。複数のアップデート情報がある場合は、再度ソフトウェアアップデートの操作を行ってください。

チェック

ソフトウェアアップデートに失敗した場合は、エラー画面が表示されます。Express5800/SG300のソフトウェアの状態はアップデートを行う前の状態に戻ります。

バックアップ

万一の障害や災害に備え、管理者はExpress5800/SG300に設定したファイアウォールの各種情報を定期的にバックアップする必要があります。必要な時に保存しておいたバックアップデータをリストアすれば、バックアップを取得した時点の状態にExpress5800/SG300を戻すことができます。

バックアップの取得

バックアップには、ルールやグループ情報などのデータのバックアップを取得する方式と、ファイアウォール機能全体を通してのバックアップを取得する方式があります。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

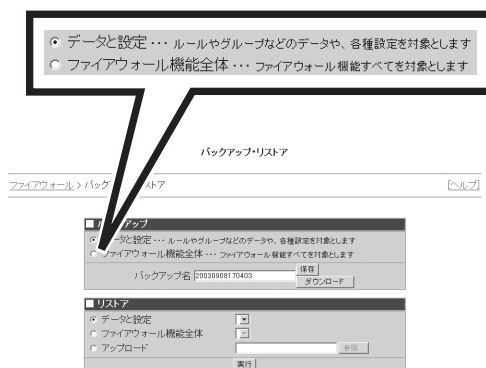
   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「システムメンテナンス」から[バックアップ・リストア]をクリックする。

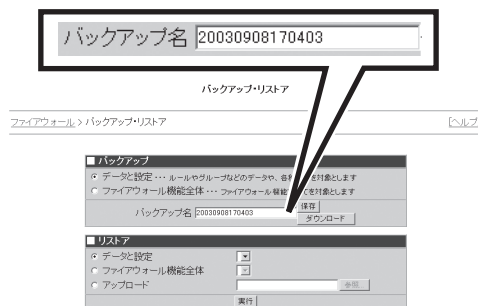
   バックアップ取得およびリストア画面が表示されます。

ファイアウォールメニュー画面

3. バックアップの方式を選択する。

   - データと設定
     ファイアウォール機能の各種設定ファイルとデータベース情報を取得します。
   - ファイアウォール機能全体
     「データと設定」で取得するバックアップデータに加えて、システムの基本設定を除くファイアウォールコンポーネントのバイナリを取得します。

バックアップ・リストア画面

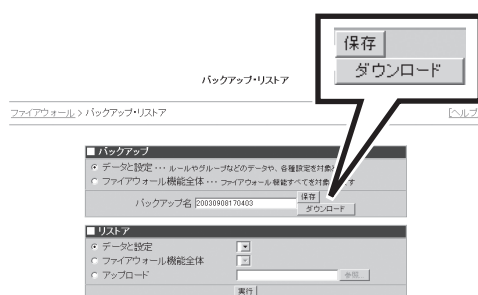
4. 「バックアップ名」を入力する。

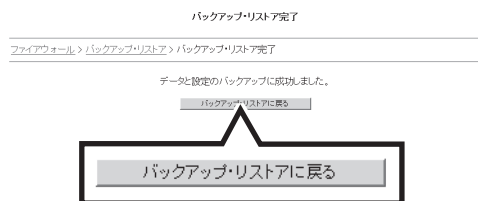
ここで入力した名前でバックアップデータは保存されます。

バックアップ・リストア画面

5. ［保存］または［ダウンロード］をクリックする。

- 保存
  取得したバックアップデータをExpress5800/SG300上に保存します。
- ダウンロード
  取得したバックアップデータを管理者が操作する管理クライアント上に保存します。

保存に成功すると、保存結果画面が表示されます。

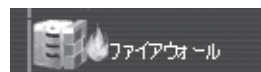
バックアップデータの取得に失敗した場合は、エラー内容を示す画面が表示されます。

バックアップ・リストア画面

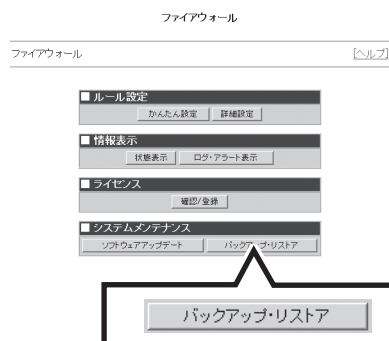
6. ［バックアップ・リストアに戻る］をクリックする。

バックアップ・リストア完了画面

バックアップのリストア

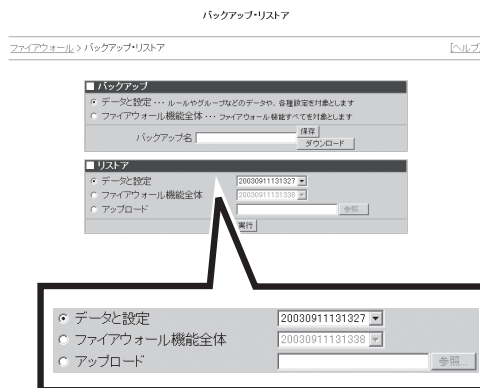
必要な時にバックアップデータをリストアすることで、Express5800/SG300をバックアップデータを取得した時点の状態に戻すことができます。

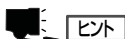
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   「ファイアウォール」メニュー画面が表示されます。

2. 「ファイアウォール」メニューの「システムメンテナンス」から[バックアップ・リストア]をクリックする。

   バックアップ取得およびリストア画面が表示されます。

ファイアウォールメニュー画面

3. リストアするバックアップデータを選択する。

   - データと設定
     ファイアウォール機能の各種設定ファイルとデータベース情報をリストアします。
   - ファイアウォール機能全体
     「データと設定」で取得するバックアップデータに加えて、システムの基本設定を除くファイアウォールコンポーネントのバイナリをリストアします。
   - アップロード
     管理者が操作する管理クライアント上に保存したバックアップデータをリストアします。

バックアップ・リストア画面

4. 「データと設定」、「ファイアウォール機能全体」を選択した場合は、バックアップデータの名前をプルダウンメニューから選択し、「アップロード」を選択した場合は入力フィールドに入力することで、リストアするバックアップデータを指定する。

ヒント

入力フィールドに入力する場合、[参照]をクリックしてデータを指定することもできます。

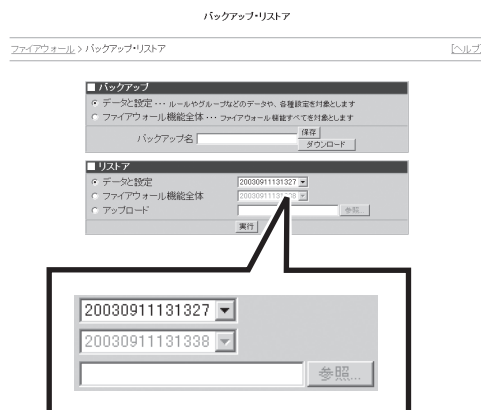
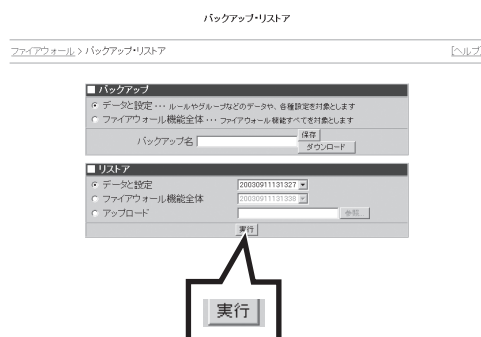
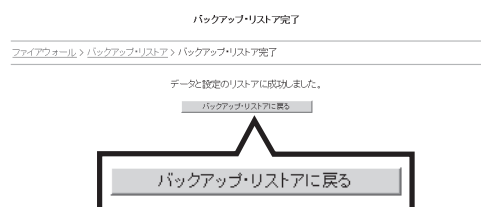
重要

管理クライアント上に取得したバックアップデータをリストアする場合は、「データと設定」に含まれるバックアップデータをリストアするか、「ファイアウォール機能全体」に含まれるバックアップデータをリストアするのかは、Express5800/SG300が自動的に判別するため、指定する必要はありません。

バックアップ・リストア画面

5. [実行]をクリックする。

バックアップデータのリストアが実行され完了すると、リストア結果画面が表示されます。

リストアに失敗した場合は、エラー内容を示す画面を表示します。

バックアップ・リストア画面

6. [バックアップ・リストアに戻る]をクリックする。

バックアップ・リストア完了画面

ユーザ認証

ここでは、ユーザが端末からExpress5800/SG300を越えて通信を行う場合のユーザ認証について説明します。

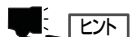
ユーザ認証 .... Express5800/SG300を利用してネットワークにアクセスするユーザの管理を行うことができます。

ユーザパスワードの変更 .... ユーザが認証時のパスワードを変更することができます。パスワードを変更するとExpress5800/SG300が管理するユーザ情報の内容も更新されます。

ユーザ認証

かんたん設定ウィザードまたは認証設定で「ユーザ認証を利用する」と設定した場合、ユーザ認証機能を利用できるようになります。ユーザ認証機能を利用した場合、ユーザごとのアクセス制御が可能になります。かんたん設定ウィザードについては、95ページの「かんたん設定ウィザード」を、「認証設定」については231ページを参照してください。ここでは、ユーザのログイン操作について説明します。

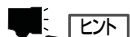
1. ブラウザで、Express5800/SG300が持つIPアドレスを、「https://」に続けて指定する。

   ヒント

   かんたん設定の「ユーザ認証の利用の設定」で、「内部ネットワークからのみ許可する」を選択している場合は、Express5800/SG300が持つ内部ネットワークに属するIPアドレスを指定する必要があります。またこの場合、アクセス元は内部ネットワークからである必要があります。

2. 上記URLに続けてユーザ認証のウェブのポート番号を指定する。

   このポート番号は、かんたん設定ウィザードで設定したものを指定します。

   例）

   ヒント

   ポート番号が443番（デフォルト設定）の場合は、番号を省略することが可能です。

   ユーザログイン画面が表示されます。

3. 画面に従い「ユーザID」、「パスワード」を入力し、[ログイン]ボタンをクリックする。

認証要求がExpress5800/SG300に送られ、Express5800/SG300は自身が管理するユーザ情報と照らし合わせて、正しいユーザによるログインであるか認証します。

ユーザログイン

ユーザログイン

■ ユーザログイン

ユーザID

パスワード

ログイン　パスワード変更

ユーザログイン画面

4. 正しいユーザであることが認証されると、ユーザログイン成功画面が表示される。

ユーザログイン結果

ユーザログイン >ログイン結果

下記ユーザのログインに成功しました。

利用できるサービスが追加されました。

■ ユーザログイン

ユーザID　test01

ユーザログインに戻る

ユーザログイン成功画面

誤ったユーザID、またはパスワードを送信した場合は、認証が失敗したことを示す画面が表示されます。認証に繰り返し失敗したユーザアカウントは、自動的にロックアウトします。許容する単位時間あたりの失敗回数、およびロックアウトの継続時間については、233ページの「ロックアウト設定」を参照してください。

重要

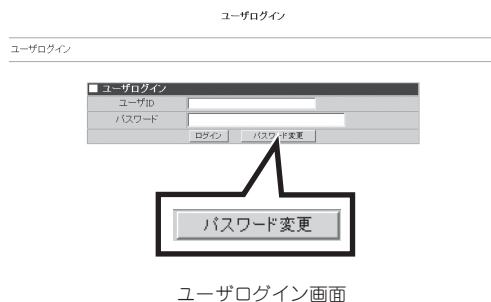
ユーザが所属するグループのルールが設定されている場合、ユーザログインに成功すると、グループルールが有効化されます。有効化されたルールは、そのユーザのセッションが終了したとしても、そのルールに定められた有効期限の間、適用されたままとなります。

ユーザパスワードの変更

ユーザログイン画面からパスワードを変更することができます。ここでは、ユーザが各自のパスワードを変更する操作について説明します。

1. URLおよびポート番号を指定し、ユーザログイン画面を表示させる。

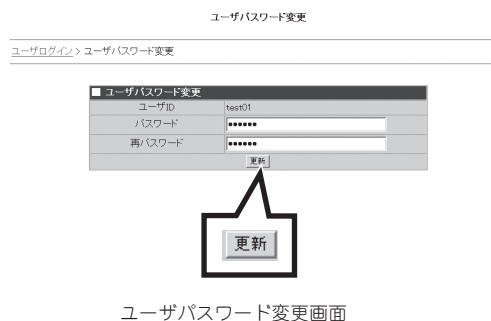
2. ユーザID、パスワードを入力し、[パスワード変更]をクリックする。

   ユーザパスワード変更画面が表示されます。

ユーザログイン画面

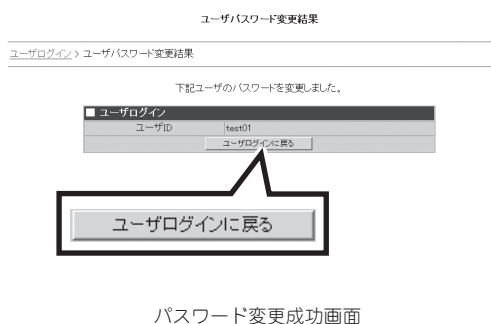
3. 「パスワード」、「再パスワード」に新しいパスワードを入力し、[更新]をクリックする。

   Express5800/SG300が新しいパスワードデータを受け取ると、管理しているユーザ情報において該当ユーザのパスワード情報の更新を行います。パスワードの変更に成功した場合は、ユーザの端末にパスワード変更成功画面を表示します。

パスワード変更に失敗した場合は、変更に失敗したことを示す画面を表示します。

ユーザパスワード変更画面

4. [ユーザログインに戻る]をクリックする。

   ユーザログイン画面が表示されます。新しいパスワードでログインしてください。

パスワード変更成功画面

5 保守・管理ソフトウェア

システム監視・管理をするための専用ソフトウェアについて説明しています。

EXPRESSBUILDER(SE)

EXPRESSBUILDER（SE：Special Edition）は、本装置を保守・管理するための統合ソフトウェアです。

起動方法

本体のCD-ROMドライブにEXPRESSBUILDER（SE）をセットして、電源をONにすると起動します。

Windowsマシンに EXPRESSBUILDER（SE）CD-ROMをセットすると管理アプリケーションのインストールやドキュメントの閲覧ができる「マスターコントロールメニュー」が表示されます。

起動方法には管理PCと本体の接続の状態により、次の3つの方法があります。

本体にコンソールを接続しての起動

次の手順に従って起動してください。

1. 本体にキーボードとディスプレイ装置を接続する。
2. 本体のCD-ROMドライブに「EXPRESSBUILDER（SE）」CD-ROMをセットする。
3. 本体の電源をOFF/ONしてシステムを再起動する。

リブート後、管理PCの画面上にメインメニューが表示され、各種保守・管理ツールを管理PCから実行できるようになります。

LAN接続された管理PCからの起動

DianaScopeを使用します。詳しくはEXPRESSBUILDER（SE）CD-ROM内の「DianaScopeオンラインドキュメント」を参照してください。

ダイレクト接続(COM B)された管理PCからの起動

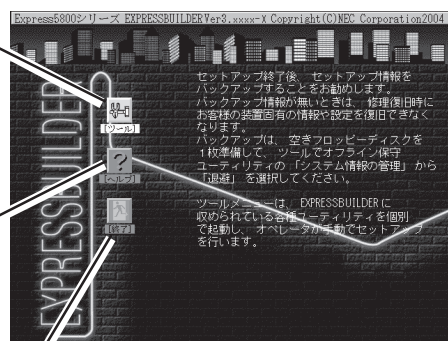
DianaScopeを使用します。詳しくはEXPRESSBUILDER（SE）CD-ROM内の「DianaScopeオンラインドキュメント」を参照してください。

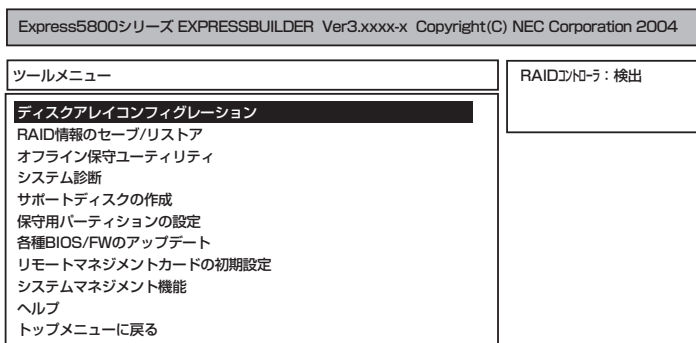
EXPRESSBUILDER(SE)トップメニュー

EXPRESSBUILDER(SE)トップメニューは各種ユーティリティを個別に起動し、オペレータによるセットアップを行うときに使用します。

BIOSの設定を間違えると、CD-ROMから起動しない場合があります。EXPRESSBUILDER(SE)を起動できない場合は、BIOS SETUPユーティリティを起動して以下のとおりに設定してください。

「Boot」メニューで「CD-ROM Drive」を一番上に、「Removable Devices」を二番目に設定する。

EXPRESSBUILDER(SE)トップメニューは以下のメニューで構成されています。

ツールメニュー

ツールメニューは、EXPRESSBUILDER(SE)に収められている各種ユーティリティを個別で起動し、オペレータが手動でセットアップを行います。
また、システム診断やサポートディスクの作成、保守用パーティションの設定を行う場合も、ツールメニューを使用します。次にツールメニューにある項目について説明します。

● **ディスクアレイコンフィグレーション**

ディスクアレイコントローラに接続されているハードディスク責に応じて自動的に論理ドライブ(ロジカルドライブ)を作成するユーティリティです。

ディスクアレイコントローラにハードディスクを接続してRAIDの新規設定や再設定を行う場合、および既存のコンフィグレーション情報をクリアする場合に使用します。

本ユーティリティでRAIDの設定を行う場合、ディスクアレイコントローラに接続するハードディスクの容量はすべて同じで、かつREADY状態である必要があります。

手順については、320ページの「ディスクアレイコンフィグレーション」を参照してください。

このメニューはRAIDを構築したときにのみ表示されます。

● **RAID情報のセーブ/リストア**

ディスクアレイシステムのコンフィグレーション情報をフロッピーディスクに保存 (セーブ)、または、フロッピーディスクから復元(リストア)することができます。

－ RAID情報のセーブ

ディスクアレイコントローラのコンフィグレーション情報をフロッピーディスクに保存します。フォーマット済みのフロッピーディスクを用意してください。RAIDの設定や変更を行った時は、必ず本機能を使用してコンフィグレーション情報をセーブしてください。

－ RAID情報のリストア

フロッピーディスクに保存されたコンフィグレーション情報をディスクアレイコントローラ上に復元します。「RAID情報のセーブ」で作成したフロッピーディスクを 用意してください。コンフィグレーション情報が万一破壊された場合や、誤ってコンフィグレーション情報を変更してしまった場合は、本機能を使用してコンフィグレーション情報をリストアしてください。

この機能は保守用です。保守以外の目的で操作しないでください。誤った操作を行うとデータを損失するおそれがあります。

● **オフライン保守ユーティリティ**

オフライン保守ユーティリティは、予防保守、障害解析を行うためのユーティリティです。ESMPROが起動できないような障害が起きた場合は、オフライン保守ユーティリティを使って障害原因の確認ができます。

● **システム診断**

本体上で各種テストを実行し、本体の機能および本体と拡張ボードなどとの接続を検査します。

本機能は、ダイレクト接続(COM B)からの実行はできますが、LAN接続での実行はできません。また、ネットワークへの影響を防止するためにも本体に接続しているネットワークケーブルはすべて取り外しておいてください。

● **サポートディスクの作成**

サポートディスクの作成では、EXPRESSBUILDER(SE)内のユーティリティをフロッピーディスクから起動するための起動用サポートディスクを作成します。なお、画面に表示されたタイトルをフロッピーディスクのラベルへ書き込んでおくと、後々の管理が容易です。

サポートディスクを作成するためのフロッピーディスクはお客様で用意してください。

- ROM-DOS起動ディスク

  ROM-DOSシステムの起動用サポートディスクを作成します。

- オフライン保守ユーティリティ

  オフライン保守ユーティリティの起動用サポートディスクを作成します。

- システムマネージメント機能

  BMC(Baseboard Management Controller)による通報機能や管理PCからのリモート制御機能を使用するための設定を行うプログラムの起動用サポートディスクを作成します。

● **保守用パーティションの設定**

ここでは、保守用パーティションに対するメンテナンスをすることができます。保守用パーティションが作成されていないときは「保守用パーティションの作成」と「FDISKの起動」以外の項目は表示されません。

重要 **「保守用パーティションの設定」の各項目を実行している間は、本体をリセットしたり、電源をOFFにしたりしないでください。**

- 保守用パーティションの作成

  保守用として内蔵ハードディスク上に領域を確保し、続けて各種ユーティリティのインストールを行います。すでに保守用パーティションが確保されている場合は、各種ユーティリティのインストールのみを行います。

- 各種ユーティリティのインストール

  各種ユーティリティ(システム診断/システムマネージメント機能/オフライン保守ユーティリティ)を、CD-ROMから保守用パーティションへインストールします。インストールされたユーティリティは、オフライン保守ユーティリティをハードディスクから起動した場合に、使用することができます。

- 各種ユーティリティの更新

  各種ユーティリティ(システム診断/オフライン保守ユーティリティ)を、フロッピーディスクから保守用パーティションへコピーします。各種ユーティリティがフロッピーディスクでリリースされたときに実行してください。それ以外では、本項目は使用しないでください。

- FDISKの起動

  ROM-DOSシステムのFDISKコマンドを起動します。パーティションの作成/削除などができます。

- **各種BIOS/FWのアップデート**

  インターネットの「NEC 8番街」で配布される「各種BIOS/FWのアップデートモジュール」を使用して、本装置のBIOSやファームウェア（FW）をアップデートすることができます。「各種BIOS/FWのアップデートモジュール」については、次のホームページに詳しい説明があります。

  『NEC 8番街』：http://nec8.com/

  各種BIOS/FWのアップデートを行う手順は配布される「各種BIOS/FWのアップデートモジュール」に含まれる「README.TXT」に記載されています。記載内容を確認した上で、記載内容に従ってアップデートしてください。「README.TXT」はWindowsのメモ帳などで読むことができます。

  重要 **BIOS/FWのアップデートプログラムの動作中は本体の電源をOFFにしないでください。アップデート作業が途中で中断されるとシステムが起動できなくなります。**

- **リモートマネージメントカードの初期設定**

  リモートマネージメントカードへの本体装置固有情報の設定を行います。本設定を行うことで、リモートマネージメントカードによるハードウェア障害の監視や障害通報、およびLAN経由/WAN経由でのリモート制御（本体装置のリセット、電源ON/OFF、システムイベントログ（SEL）の確認など）が可能となります。

- **システムマネージメント機能**

  通報機能、リモート制御機能を使用するための設定を行います。

- **ヘルプ**

  EXPRESSBUILDER（SE）の各種機能に関する説明を表示します。

- **終了**

  EXPRESSBUILDER（SE）を終了します。

コンソールレスメニュー

EXPRESSBUILDER(SE)は、本装置にキーボードなどのコンソールが接続されていなくても各種セットアップを管理用コンピュータ(管理PC)から遠隔操作することができる「コンソールレス」機能を持っています。

重要

- **本装置以外のコンピュータおよびEXPRESSBUILDER(SE)が添付されていた本装置以外のExpress5800シリーズに使用しないでください。故障の原因となります。**
- **コンソールレス時の使用は、本体にキーボードが接続されていないことが条件です。本体にキーボードが接続されていると、EXPRESSBUILDER(SE)はコンソールがあると判断し、コンソールレス動作を行いません(管理PCにメニューを表示しません)。**

起動方法

起動方法には管理PCと本体の接続状態により、次の2つの方法があります。

- LAN接続された管理PCから実行する
- ダイレクト接続(シリアルポートB)された管理PCから実行する

起動方法の手順については、「DianaScopeオンラインドキュメント」を参照してください。

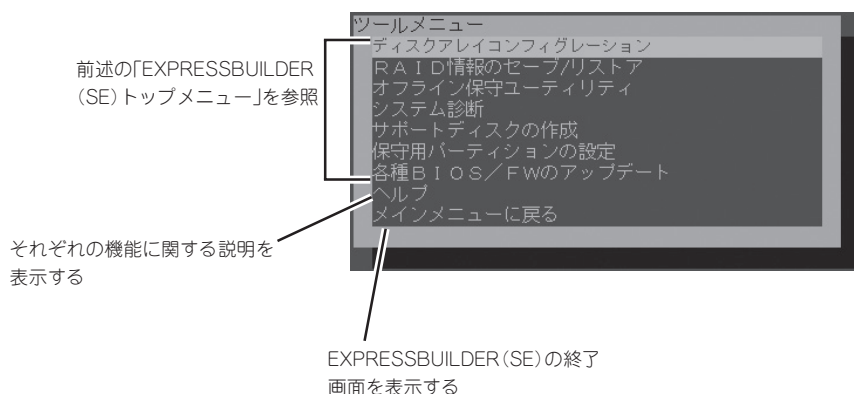
- **BIOSセットアップユーティリティのBootメニューで起動順序を変えないでください。CD-ROMドライブが最初に起動するようになっていないと使用できません。**
- **LAN接続はLANポート1のみ使用可能です。**
- **ダイレクト接続はシリアルポートBのみ使用可能です。**
- **コンソールレスで本装置を遠隔操作するためには、設定情報を格納したフロッピーディスクが必要になります。**

  フォーマット済みのフロッピーディスクを用意しておいてください。
- **BIOS SETUPを通常の終了方法以外の手段(電源OFFやリセット)で終了するとリダイレクションが正常にできない場合があります。設定ファイルで再度設定を行ってください。**

BIOS設定情報は以下の値にセットされます。

ーLAN #1:	[Enabled]
ーSerial Port A:	[Enabled]
ーSerial Port A I/O Address:	[3F8]
ーSerial Port A Interrupt:	[IRQ 4]
ーSerial Port B:	[Enabled]
ーSerial Port B I/O Address:	[2F8]
ーSerial Port B Interrupt:	[IRQ 3]
ーBIOS Redirection Port:	[Serial Port B]
ーBIOS Redirection Baud Rate:	[19.2k]
ーBIOS Redirection Flow Control:	[CTS/RTS]
ーConsole Type:	[PC ANSI]

ツールメニュー

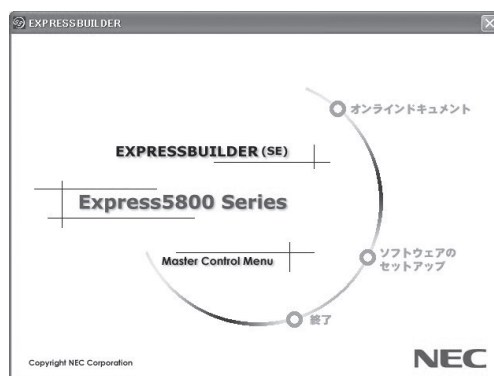
メインメニューでツールを選択すると以下のメニューが表示されます。

「EXPRESSBUILDER(SE)トップメニュー」の「ツールメニュー」にある機能と比較すると「システム診断」の内容や操作方法が異なります。詳しくは、この章の「システム診断」を参照してください。

メニュー（機能）については、前述の「EXPRESSBUILDER（SE）トップメニュー」と同じです。前述の説明を参照してください。

マスターコントロールメニュー

Windows 95以降、またはWindows NT 4.0以降が動作しているコンピュータ上で添付のCD-ROM「EXPRESSBUILDER(SE)CD-ROM」をセットすると、「マスターコントロールメニュー」が自動的に起動します。

システムの状態によっては自動的に起動しない場合があります。そのような場合は、CD-ROM上の次のファイルをエクスプローラ等から実行してください。

CD-ROMのドライブレター：¥MC¥1ST.EXE

マスターコントロールメニューからは、リモート管理ユーティリティである「EMSPRO/SeverManager」や「DianaScope」のインストールやオンラインドキュメントを参照することができます。終了する場合は、[終了]をクリックしてください。

オンラインドキュメントの中には、PDF形式の文書で提供されているものもあります。このファイルを参照するには、あらかじめAdobeシステムズ社製のAcrobat Readerがインストールされている必要があります。Acrobat Reader がインストールされていないときは、はじめに[ソフトウェアのセットアップ]の[Acrobat Reader]を選択して、Acrobat Readerをインストールしておいてください。

マスターコントロールメニューの操作は、ウィンドウに表示されているそれぞれの項目をクリックするか、右クリックして現れるショートカットメニューを使用してください。また、一部のメニュー項目は、メニューが動作しているシステム・権限で実行できないとき、グレイアウト表示され選択できません。適切なシステム・権限で実行してください。

重要

CD-ROMをドライブから取り出す前に、マスターコントロールメニューおよびメニューから起動されたオンラインドキュメント、各種ツールは終了させておいてください。

ディスクアレイコンフィグレーション

ディスクアレイコンフィグレーションはディスクアレイコントローラに接続されているハードディスク責に応じて自動的に論理ドライブ(ロジカルドライブ)を作成するユーティリティです。

ディスクアレイコントローラにハードディスクを接続してRAIDの新規設定・再設定を行う場合、および既存のコンフィグレーション情報をクリアする場合に使用します。

使用上の注意

ディスクアレイコンフィグレーションを実行する前にお読みください。

- RAIDを構築するハードディスクドライブは同じ容量、同じ回転数のものを使用してください。
- コンフィグレーション済みのディスクアレイコントローラを使用する場合、新規に論理ドライブを作成する前に、既存のコンフィグレーション情報をクリアする必要があります。コンフィグレーション情報をクリアすると、既存のデータは失われますのでご注意ください。
- 本ユーティリティでRAIDの設定を行う場合、ディスクアレイコントローラに接続するハードディスクの容量はすべて同じで、かつREADY状態である必要があります。
- 本ユーティリティでは、指定されたハードディスク構成で割り当て可能な最大容量を使用し、単一の論理ドライブを作成することができます。また、論理ドライブの容量を任意で指定することにより、複数の論理ドライブ(最大4台)を作成することもできます。
- RAIDの設定を行う場合は、本装置がサポートしているRAID構成を指定してください。通常は、指定されたハードディスク構成で割り当て可能な最大容量を使用し、単一の論理ドライブを作成します。複数の論理ドライブ作成の指示がある場合のみ、容量を指定して作成してください。
- RAIDの新規設定、再設定を行った場合、コンフィグレーション情報をフロッピーディスクに保存してください。手順は、314ページの「RAID情報のセーブ/リストア」を参照してください。
- 本体のマザーボード上にあるSATAインタフェースに接続したハードディスクドライブに対する設定をする場合は、このメニューを起動する前に6章の「システムBIOSのセットアップ」を参照して「SATA RAID Enable」の設定を有効にしてください。

使用方法

以下の手順でディスクアレイコンフィグレーションを起動し、操作します。

1. 6章の「システムBIOSのセットアップ」を参照して「SATA RAID Enable」の設定を有効にする。

2. EXPRESSBUILDER(SE)CD-ROMからシステムを起動する。

   EXPRESSBUILDER(SE)の起動方法は、312ページの「EXPRESSBUILDER(SE)」を参照してください。
   管理PCの画面にメインメニューが表示されます。

3. メインメニューから「ディスクアレイコンフィグレーション」を選択する。

   ユーティリティが起動し、ディスクアレイコントローラに接続されたハードディスクの状態と論理ドライブの状態をチェックします。

   すでに論理ドライブが存在する場合やREADY状態以外の物理ディスクが存在する場合、現在のコンフィグレーション情報をクリアするかどうかの確認のメッセージが表示されます。

   - 「Y」を選択した場合

     コンフィグレーション情報をクリアした後、設定可能なRAID構成が表示されます。

   - 「N」を選択した場合

     ユーティリティを終了します。

4. 設定したいRAID構成を選択し、番号を入力する。

   作成する論理ドライブの各種パラメータが表示され、確認メッセージが表示されます。

   - 表示された内容で論理ドライブを作成する場合

     「Y」を選択します。
     自動的に論理ドライブの作成、および初期化を開始します。

   - 論理ドライブの容量を変更する場合

     「S」を選択します。
     容量は画面上に表示される入力指定範囲内(MB単位)で指定します。容量の入力が完了したら、再度、作成する論理ドライブの確認メッセージが表示されます。入力した値が 画面上に表示されていることを確認し、「Y」を選択します。
     自動的に論理ドライブの作成、および初期化を開始します。

     複数の論理ドライブを作成する場合はこの手順を繰り返します。

   - RAID構成を再指定する場合

     「N」を選択します。
     論理ドライブをまだ作成していない場合は、RAID構成の再指定が可能です。
     論理ドライブを1台以上作成している場合は、「N」を選択するとユーティリティは終了します。

以上で、ディスクアレイコンフィグレーションは終了です。

オフライン保守ユーティリティ

オフライン保守ユーティリティは、本製品の予防保守、障害解析を行うためのユーティリティです。ESMPROが起動できないような障害が本製品に起きた場合は、オフライン保守ユーティリティを使って障害原因の確認ができます。

重要

- **オフライン保守ユーティリティは通常、保守員が使用するプログラムです。オフライン保守ユーティリティを起動すると、メニューにヘルプ(機能や操作方法を示す説明)がありますが、無理な操作をせずにオフライン保守ユーティリティの操作を熟知している保守サービス会社に連絡して、保守員の指示に従って操作してください。**
- **オフライン保守ユーティリティが起動すると、クライアントから本製品にアクセスできなくなります。**

オフライン保守ユーティリティの起動方法

オフライン保守ユーティリティは次の方法で起動することができます。

- EXPRESSBUILDER(SE)からの起動

  「EXPRESSBUILDER(SE)トップメニュー」から「ツール」ー「オフライン保守ユーティリティ」の順に選択すると、CD-ROMよりオフライン保守ユーティリティが起動します。

- フロッピーディスクからの起動

  「EXPRESSBUILDER(SE)トップメニュー」の「ツール」ー「サポートディスクの作成」で作成した「オフライン保守ユーティリティ起動FD」をセットして起動すると、オフライン保守ユーティリティが起動します。

- 手動起動(F4キー)

  オフライン保守ユーティリティをインストール後、POST画面で<F4>キーを押すと、ディスクよりオフライン保守ユーティリティが起動します。

オフライン保守ユーティリティの機能

オフライン保守ユーティリティを起動すると、以下の機能を実行できます(起動方法により、実行できる機能は異なります)。

- **IPMI情報の表示**

  IPMI(Intelligent Platform Management Interface)におけるシステムイベントログ(SEL)、センサ装置情報(SDR)、保守交換部品情報(FRU)の表示やバックアップをします。

  本機能により、本製品で起こった障害や各種イベントを調査し、交換部品を特定することができます。

- **BIOSセットアップ情報の表示**

  BIOSの現在の設定値をテキストファイルへ出力します。

- **システム情報の表示**

  プロセッサ(CPU)やBIOSなどに関する情報を表示したり、テキストファイルへ出力したりします。

- **システム情報の管理**

  お客様の装置固有の情報や設定のバックアップ(退避)をします。バックアップをしておかないと、ボードの修理や交換の際に装置固有の情報や設定を復旧できなくなります。

システム情報のバックアップの方法については、72ページで説明しています。なお、リストア(復旧)は操作を熟知した保守員以外は行わないでください。

- **各種ユーティリティの起動**

  「EXPRESSBUILDER(SE) CD-ROM」から保守用パーティションにインストールされた以下のユーティリティを起動することができます。

  - システムマネージメント機能
  - システム診断ユーティリティ
  - 保守用パーティションの設定

- **筐体識別**

  本装置のランプ、ブザーなどで、本装置を識別できるようにします。ラックに複数台の装置が設置された局面で装置を識別するときなどに便利です。

システム診断

システム診断は装置に対して各種テストを行います。
EXPRESSBUILDER(SE)の「ツール」メニューから「システム診断」を実行して診断してください。

システム診断の内容

システム診断には、次の項目があります。

- メモリのチェック
- CPUキャッシュメモリのチェック
- システムとして使用されているハードディスクドライブのチェック

システム診断を行う時は、必ず本体に接続しているネットワークケーブルを外してください。接続したままシステム診断を行うと、ネットワークに影響をおよぼすおそれがあります。

ハードディスクドライブのチェックでは、ディスクへの書き込みは行いません。

システム診断の起動と終了

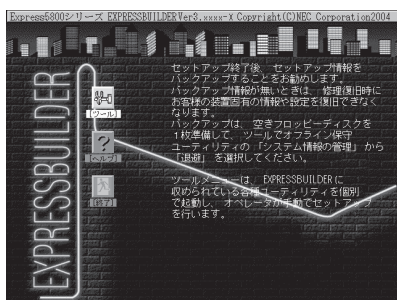
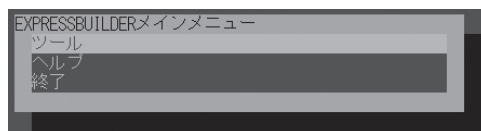
システム診断には、本体に直接接続されたコンソール(キーボード)を使用する方法と、本体前面のCOM Bポートとダイレクト接続された管理PCのコンソールを使用する方法(コンソールレス)があります。それぞれの起動方法は次の通りです。

EXPRESSBUILDER(SE)のコンソールレスでの起動方法には、ダイレクト接続(COM B)とLAN接続の2つの方法がありますが、システム診断はダイレクト接続(COM B)でしか利用することができません。

1. シャットダウン処理を行った後、本体の電源をOFFにし、電源コードをコンセントから抜く。
2. 本体に接続しているネットワークケーブルをすべて取り外す。
3. 電源コードをコンセントに接続し、本体の電源をONにする。

4. 「EXPRESSBUILDER（SE） CD-ROM」からシステムを起動する。

本体のコンソールを使用して起動する場合と、コンソールレスで起動する場合で手順が異なります。本章の「EXPRESSBUILDER(SE)」を参照して正しく起動してください。

EXPRESSBUILDER(SE)から起動すると画面にメニューが表示されます。本体のコンソールを使用して起動した場合は、本体に接続しているディスプレイ装置に「EXPRESSBUILDER(SE)トップメニュー」が表示されます。コンソールレスで起動した場合は、管理PCのディスプレイに「EXPRESSBUILDER(SE)メインメニュー」が表示されます。

EXPRESSBUILDER(SE)トップメニュー

EXPRESSBUILDER(SE)メインメニュー

5. ［ツール］を選択する。

6. ［ツールメニュー］の［システム診断］を選択する。

システム診断を開始します。約3分で診断は終了します。
診断を終了するとディスプレイ装置の画面が次のような表示に変わります。

試験タイトル

TeDoLi (TEst & Diagnosis On Linux) Ver001.00 (Build020901.1.1m)

Test End

Start 10:06:58　End 10:09:58　Pass 000:03:00　TestTime 000:03:00
Test End:　NormalEnd　03　AbnormalEnd　00　ForceEnd　00

<System>
MEM　Memory　16 count　NormalEnd
CACHE　Cache　49 count　NormalEnd
<SCSI>
HDD_02:000　DK32DJ-36W　89 count　NormalEnd

[Enter] Detail Information　[ESC] Return to Enduser Menu

試験ウィンドウタイトル

試験結果

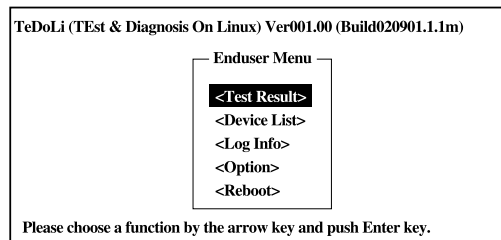
試験簡易ウィンドウ

ガイドライン

試験タイトル:　診断ツールの名称およびバージョン情報を表示します。
試験ウィンドウタイトル:診断状態を表示します。試験終了時にはTest Endと表示します。
試験結果:　診断開始・終了・経過時間および終了時の状態を表示します。
ガイドライン:　ウィンドウを操作するキーの説明を表示します。
試験簡易ウィンドウ:　診断を実行した各試験の結果を表示します。カーソル行で<Enter>キーを押すと試験の詳細を表示します。

システム診断でエラーを検出した場合は試験簡易ウィンドウの該当する試験結果が赤く反転表示し、右側の結果に「Abnormal End」を表示します。
エラーを検出した試験にカーソルを移動し<Enter>キーを押し、試験詳細表示に出力されたエラーメッセージを記録して保守サービス会社に連絡してください。

7. 画面最下段の「ガイドライン」に従い<Esc>キーを押す。

   以下のメインメニューを表示します。

   <Test Result>: 前述の診断終了時の画面を表示します。
   <Device List>: 接続されているデバイス一覧情報を表示します。
   <Log Info>: 試験ログを表示します。エラーメッセージをフロッピーディスクへ保存することができます。フロッピーディスクへ記録する場合は、フォーマット済みのフロッピーディスクをフロッピーディスクドライブにセットし、<Save>を選択してください。
   <Option>: ログの出力先の変更します。
   <Reboot>: システムを再起動します。

8. 上記メインメニューで<Reboot>を選択する。

   再起動し、システムが「EXPRESSBUILDER(SE)CD-ROM」から起動します。

9. EXPRESSBUILDER(SE)を終了し、CD-ROMドライブから「EXPRESSBUILDER(SE) CD-ROM」を取り出す。

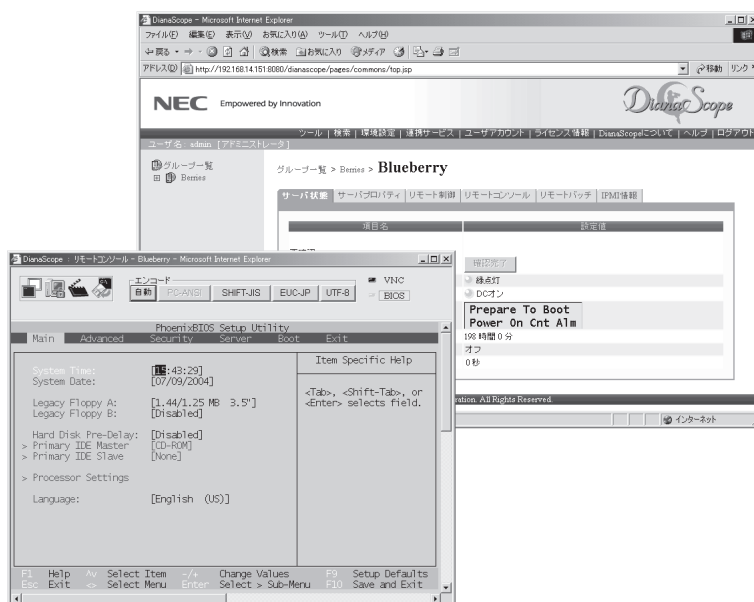
10. 本体の電源をOFFにし、電源コードをコンセントから抜く。

11. 手順2で取り外したネットワークケーブルを接続し直す。

12. 電源コードをコンセントに接続する。

以上でシステム診断は終了です。

DianaScope

DianaScopeはExpress5800シリーズをリモート管理するためのソフトウェアです。DianaScopeの機能やインストール方法についての詳細はオンラインドキュメントを参照してください。

本製品においてDianaScopeを使用するためにはオプションのサーバライセンス(UL1198-001またはUL1198-011)が必要です。本製品には以下のサーバライセンスが添付されています。

ー　UL1198-001 SystemGlobe DianaScope Additional Server License(1)

BMC Online Update

BMC Online Updateは、インターネットで配布される「BMC（Base board Management Controller）ファームウェア」を使用して、本体内に装着されているリモートマネージメントカード内のBMCファームウェアを更新するソフトウェアです。

- このソフトウェアは2MB以上の空き容量を必要とします。
- 管理PCからリモート操作する場合は、「DianaScope」を使用します。設定や通信方法についてはDianaScopeのオンラインドキュメントを参照してください。

インストール

1. rootユーザーでログイン後、EXPRESSBUILDER CD-ROMから以下のファイルを適当なディレクトリにコピーする。

   「cp/mnt/cdrom/BMCTOOL/OnlineUp/BmcOnlineUpdate.i386」

2. rpmファイルを解凍する。

   「rpm - ivh BmcOnlineUpdate. i386」

起動方法

- **BMCファームウェアの更新作業をしている間は装置の電源をOFFにしないでください。更新作業が途中で中断されるとシステムが起動できなくなります。**
- **更新されたBMCファームウェアは、装置の再起動後に有効になります。再起動を行うまでは、更新前の状態で運用を継続します。**

下記の入力を行い、プログラムを開始させてください。

```
cd /usr/BmcOnlineUpdate
. /BmcOnlineUpdate -ja
```

日本語をサポートしていない場合はオプション"-ja"をつけないでください。

./BmcOnlineUpdate

エラー表示一覧

下表にエラーメッセージと対処方法を示します。

メッセージ	対処方法
アップデートの必要がありません。	現在使用している環境は、アップデートしようとしたデータより新しいか同じデータが適用されています。
対象装置ではありません。	データが対象装置のものではありません。対象装置のデータでUpdateを実行してください。
BMC情報を取得できません。	リモートマネージメントカードが正常に取り付けられているか確認してください。取り付けを確認してからUpdateを実行してください。
オンラインモードに移行できません。	BMCがビジー状態の可能性があります。数分後に再度実行してください。
運用中のデータの退避に失敗しました。	
更新モードに移行できません。	
データの更新中にエラーが発生しました。	
終了処理に失敗しました。	
IPMIドライバが見つかりません。	IPMIドライバをインストールしてください。
サポート対象外です。	アップデート機能をサポートしていないBMCです。このツールによるアップデートはできません。

重要 **対処方法を実行しても、アップデートに失敗した場合は保守サービス会社に連絡してください。**

ESMPRO

ESMPRO/ServerAgent、ServerManagerは、システムの安定稼動と効率的なシステム運用を目的とした管理ソフトウェアです。構成情報や稼動状況を管理し、システムの異常を検出した際にシステム管理者へ通報することにより、システム障害の予防や障害に対する迅速な対処を可能にします。

添付のCD-ROM「バックアップCD-ROM」には、本体を管理するアプリケーション「ESMPRO/ServerAgent」が格納されています。ESMPRO/ServerAgentと通信を行いネットワーク上の管理PCから本装置を監視するアプリケーション「ESMPRO/ServerManager」は「EXPRESSBUILDER(SE) CD-ROM」に格納されています。

- **ESMPRO/ServerManager**

  ESMPRO/ServerManagerの動作環境やインストール方法、アンインストール方法および運用時の注意事項については「EXPRESSBUILDER(SE) CD-ROM」にある「ESMPRO/ServerManagerインストレーションガイド」を参照してください。

- **ESMPRO/ServerAgent**

  ESMPRO/ServerAgentは本装置に自動でインストールされる監視アプリケーションです。ESMPRO/ServerAgentに関する詳細な説明は本体に添付の「バックアップCD-ROM」内にあるオンラインマニュアル(PDFファイル)を参照してください。

  添付のバックアップCD-ROM:/nec/Linux/esmpro.Sa/doc

  ESMPRO/ServerAgentは出荷時のハードディスクにインストール済みです。また、再インストールの時も自動的にインストールされます。

エクスプレス通報サービス

エクスプレス通報サービスは、システムに発生する障害情報（予防保守情報含む）を電子メールで保守センターに自動通報するソフトウェアです。
本サービスを使用することにより、システムの障害を事前に察知したり、障害発生時に迅速に保守を行ったりすることができます。

エクスプレス通報サービスは出荷時のハードディスクにインストール済みです。また、再インストールの時も自動的にインストールされます。

エクスプレス通報サービスを利用するためには、別途契約が必要となります。詳しくは、お買い求めの販売店または保守サービス会社にお問い合わせください。

6 システムの拡張とコンフィグレーション

本装置がサポートしている内蔵タイプのオプションデバイスの増設方法やシステムが提供する各種機能の設定方法について説明します。

内蔵オプションの取り付け

本体に取り付けられるオプションの取り付け方法および注意事項について記載しています。

重要

- オプションの取り付け/取り外しはユーザー個人でも行えますが、この場合の本体および部品の破損または運用した結果の影響についてはその責任を負いかねますのでご了承ください。本装置について詳しく、専門的な知識を持った保守サービス会社の保守員に取り付け/取り外しを行わせるようお勧めします。
- オプションおよびケーブルは弊社が指定する部品を使用してください。指定以外の部品を取り付けた結果起きた装置の誤動作または故障・破損についての修理は有料となります。

安全上の注意

安全に正しくオプションの取り付け/取り外しをするために次の注意事項を必ず守ってください。

装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。

- 自分で分解・修理・改造はしない
- リチウムバッテリを取り外さない
- プラグを差し込んだまま取り扱わない

注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 落下注意
- 装置を引き出した状態にしない
- 中途半端に取り付けない
- カバーを外したまま取り付けない
- 指を挟まない
- 高温注意

静電気対策について

本体内部の部品は静電気に弱い電子部品で構成されています。取り付け・取り外しの際は静電気による製品の故障に十分注意してください。

- **リストストラップ(アームバンドや静電気防止手袋など)の着用**

  リスト接地ストラップを手首に巻き付けてください。手に入らない場合は部品を触る前に筐体の塗装されていない金属表面に触れて身体に蓄積された静電気を放電します。
  また、作業中は定期的に金属表面に触れて静電気を放電するようにしてください。

- **作業場所の確認**

  - 静電気防止処理が施された床、またはコンクリートの上で作業を行います。
  - カーペットなど静電気の発生しやすい場所で作業を行う場合は、静電気防止処理を行った上で作業を行ってください。

- **作業台の使用**

  静電気防止マットの上に本体を置き、その上で作業を行ってください。

- **着衣**

  - ウールや化学繊維でできた服を身につけて作業を行わないでください。
  - 静電気防止靴を履いて作業を行ってください。
  - 取り付け前に貴金属(指輪や腕輪、時計など)を外してください。

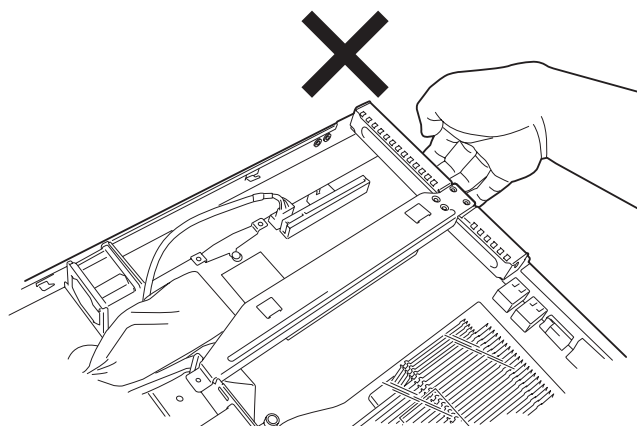
- **部品の取り扱い**

  - 取り付ける部品は本体に組み込むまで静電気防止用の袋に入れておいてください。
  - 各部品の縁の部分を持ち、端子や実装部品に触れないでください。
  - 部品を保管・運搬する場合は、静電気防止用の袋などに入れてください。

取り付け/取り外しの準備

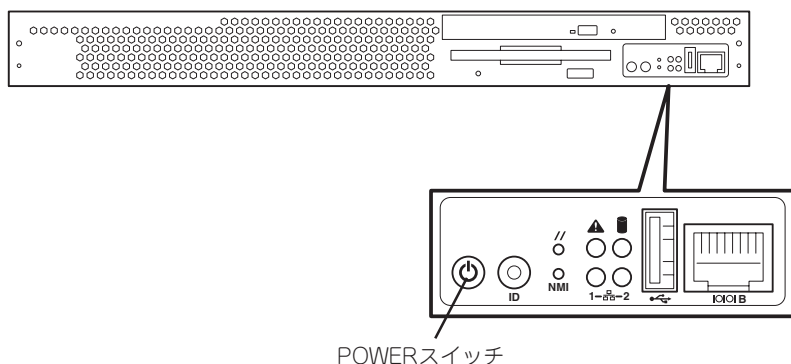
部品の取り付け/取り外しの作業をする前に準備をします。

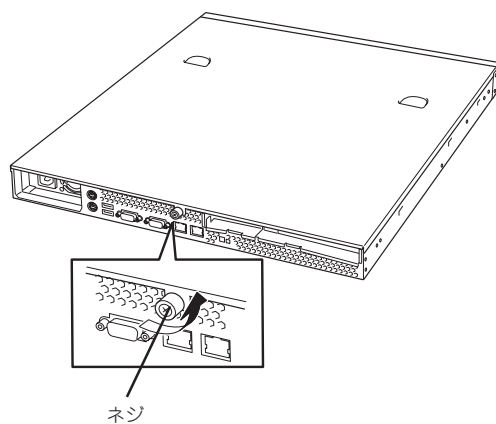
重要

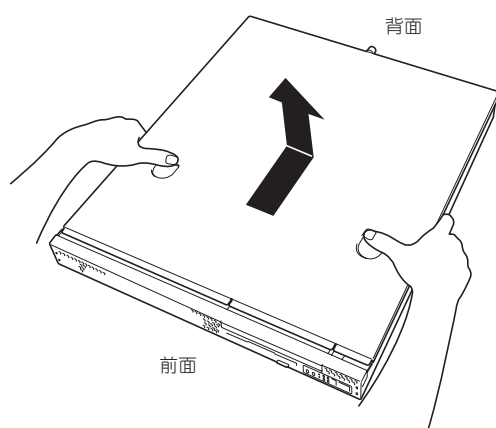
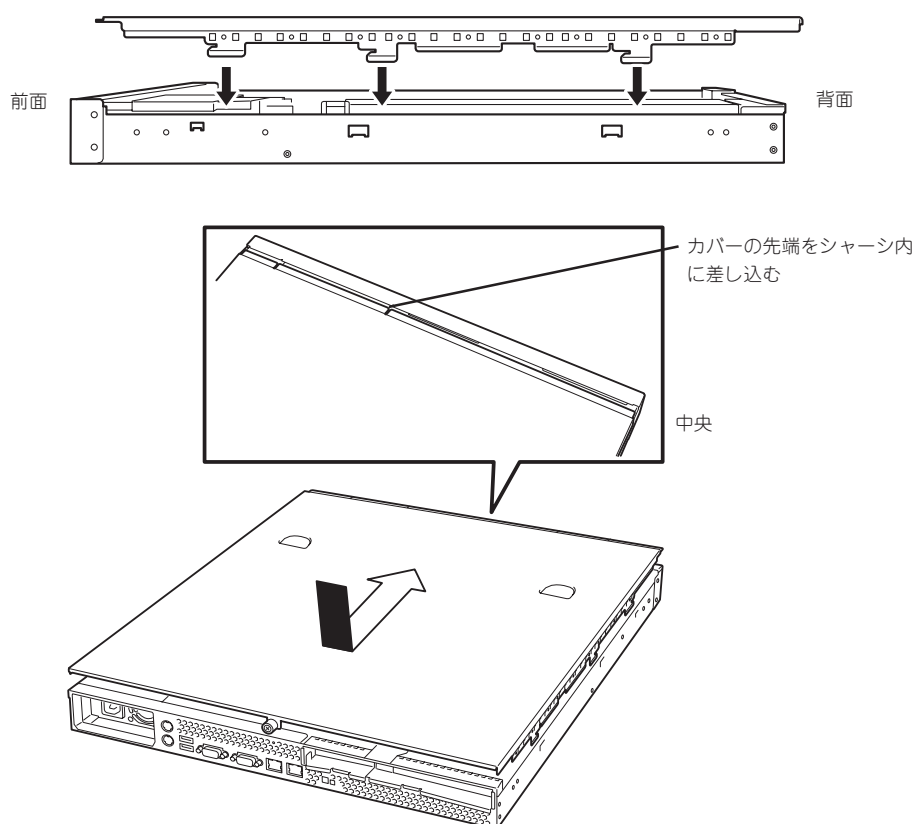
- トップカバーを取り外して準備ができた後、本体を持つときにPCIライザーを持たないでください。

- 電源コードを本体から取り外した後、約5秒ほど待ってから作業を続けてください。電源コードを取り外してから3～4秒ほどの間、マザーボード上の部品やリモートマネージメントカード(RMC)は動作を続けている場合があります。RMCの動作が完全に停止してから作業を続けてください。

卓上に設置している場合

本体を卓上に設置している場合の手順について説明します。

1. OSからシャットダウン処理をするかPOWERスイッチを押して本体の電源をOFF(POWERランプ消灯)にする。

2. 本体に接続しているすべてのケーブルおよび電源コードを取り外す。

3. 背面のネジをゆるめる。

4. トップカバーを取り外す。

   くぼみの部分に指をかけてスライドさせてから持ち上げてください。

トップカバーを取り付けるときは、トップカバーにあるフックと本体のフレームにある穴をあわせてていねいに本体に置いた後、前面へ向けてスライドさせてください。

トップカバーの取り付け後、背面のネジで本体に固定します。

ネジが締めづらいときはトップカバーを本体に軽く押し付けながら締めてください。

ラックに設置している場合

本体をラックに設置している場合の手順について説明します。ラックからの取り外しは1人でもできますが、なるべく複数名で行うことをお勧めします。

⚠ 注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **落下注意**
- **装置を引き出した状態にしない**
- **カバーを外したまま取り付けない**
- **指を挟まない**

1. フロントベセルを取り付けている場合はフロントベセルを取り外す。
2. 336ページの手順を参照して本体をラックから取り外し、じょうぶで平らな机の上に置く。

   重要

   本体を引き出したまま放置しないでください。必ずラックから取り外してください。

3. 背面のネジをゆるめる(337ページの手順3参照)。
4. トップカバーを取り外す。

   くぼみの部分に指をかけてスライドさせてから持ち上げてください(337ページの手順4参照)。

トップカバーを取り付けるときは、338ページを参照して取り付けてください。

取り付け/取り外しの手順

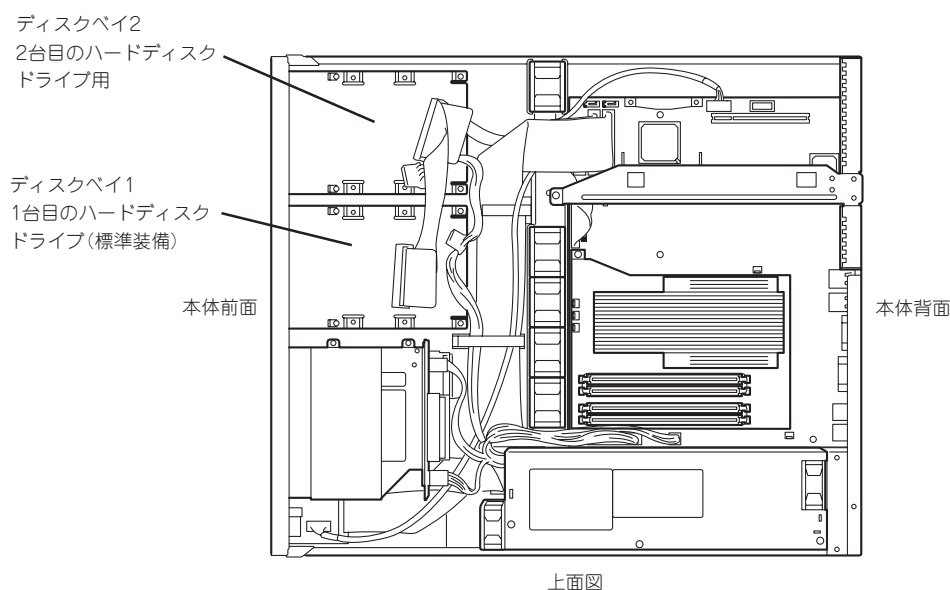
次の手順に従って部品の取り付け/取り外しをします。

ハードディスクドライブ

本体には、最大2台のハードディスクドライブを搭載することができます。

上面図

ハードディスクドライブインタフェースはシリアルATAです。

重要

- 弊社で指定していないハードディスクドライブを使用しないでください。サードパーティのハードディスクドライブなどを取り付けると、ハードディスクドライブだけでなく本体が故障するおそれがあります。次に示すモデルをお買い求めください。

  − N8150-184(80GB、7,200rpm、SATA)

- 異なるインターフェースのハードディスクドライブを混在して搭載することはできません。 また、搭載するハードディスクドライブの回転数や容量は同じものを使用してください。

- SATAハードディスクドライブ(標準装備)の場合、単体ドライブとして2台のハードディスクドライブを搭載して運用することはできません。標準装備のハードディスクドライブにハードディスクドライブを追加する場合は、2台のハードディスクドライブでディスクアレイを構築して運用します(RAID1)。RAIDを構築するためにはBIOSの「SATA RAID Enable」のパラメータを「Disabled」から「Enabled」に変更してください。

  また、標準装備のハードディスクドライブの初期化などを行うため、増設の前に大切なデータのバックアップを必ず行ってください。

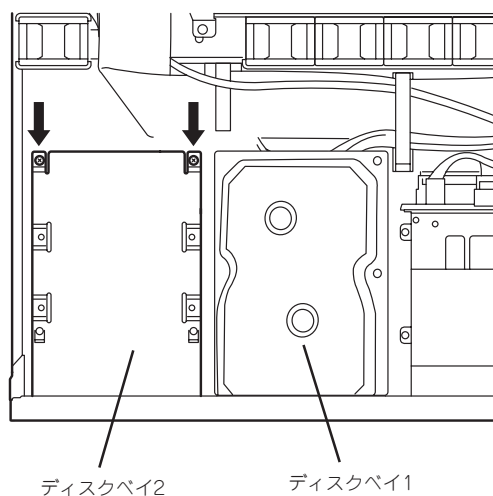
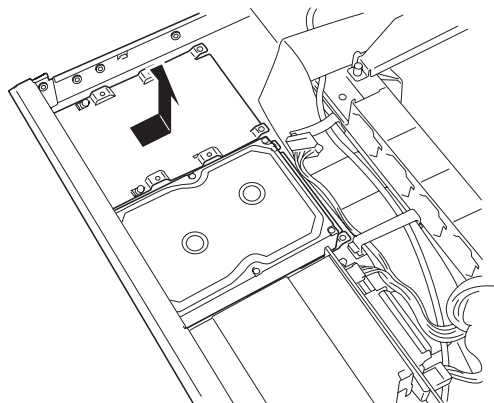
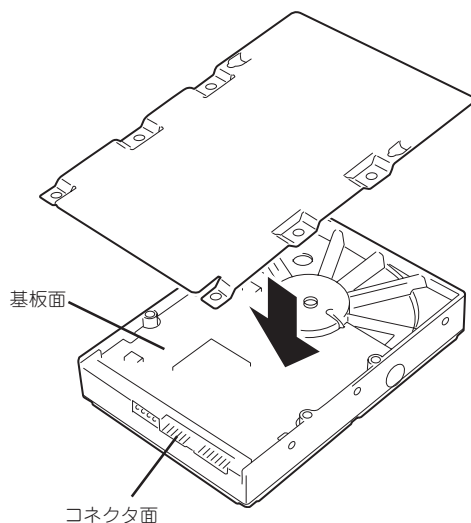
取り付け

次に示す手順でハードディスクドライブを取り付けます。

ここではディスクベイ2への取り付け手順を図で示していますがディスクベイ1への取り付けも同様の手順で行えます。

1. ハードディスクドライブ内の大切なデータのバックアップをとる。

   バックアップについては3章を参照してください。

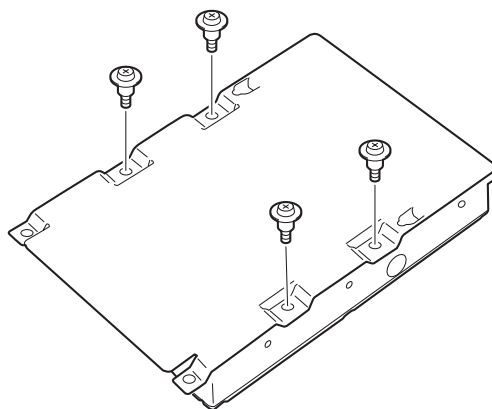
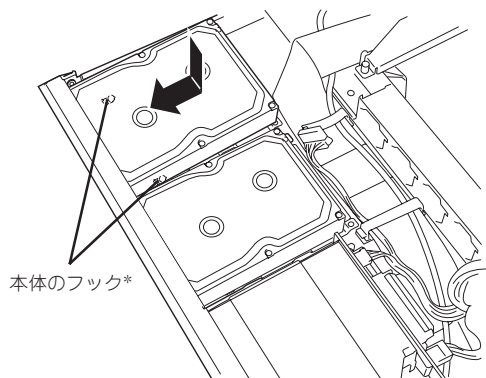
2. 336ページを参照して準備をする。
3. ディスクベイにハードディスクドライブを搭載している場合は、ハードディスクドライブに接続しているケーブルをすべて取り外す。
4. ディスクベイを固定しているネジ2本を外す。

5. ディスクベイを取り外す。

6. ハードディスクドライブの基板面を上にして置き、その上にディスクベイを静かにていねいに置く。

✔ チェック

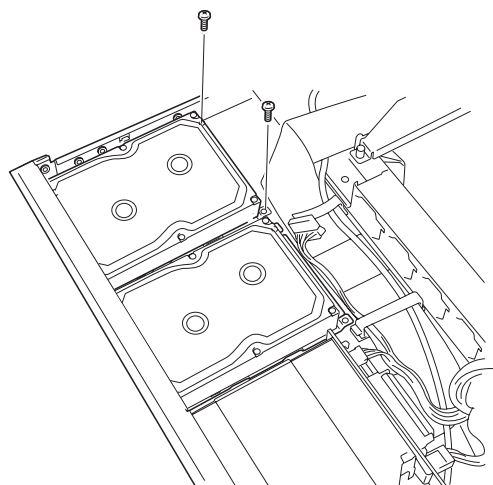
ハードディスクドライブとディスクベイの向きについて図を参照して確認してください。またハードディスクドライブとディスクベイにあるネジ穴が合っていることも確認してください。

7. 本装置に添付のネジを使ってディスクベイに固定する。

重要

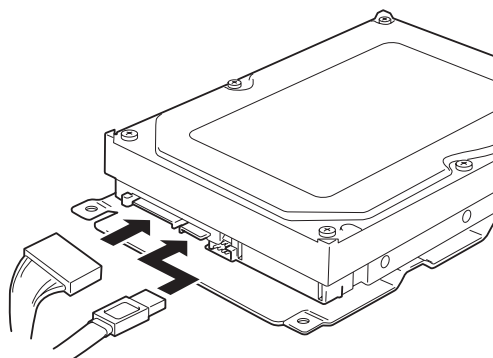
ネジは本装置に添付のネジを使用してください。

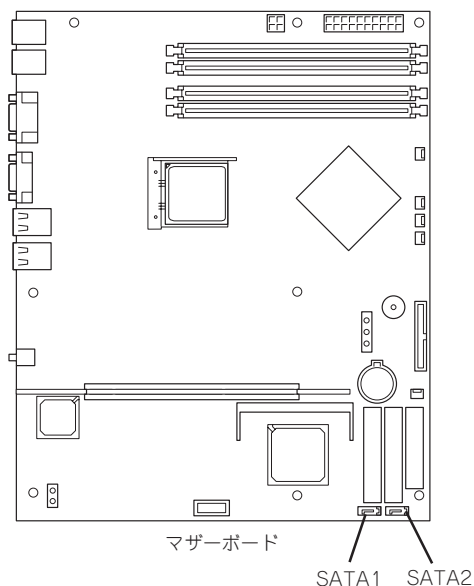
このネジは特殊なネジです。ハードディスクドライブを増設する際にこのネジが必要となるため、使用していないネジは大切に保管してください。

8. ディスクベイをしっかりと持ち、本体のフック(2個)をディスクベイの穴に通して置き、前面へスライドさせる。

* フックは各ディスクベイに2個あります。

9. 手順4で外したネジでディスクベイを固定する。

チェック

ディスクベイの取り付けの際に電源ケーブルなどを挟んでいないことを確認してください。

10. 電源ケーブルとインターフェースケーブルを接続する。

重要

電源ケーブルのコネクタにケーブルキャップが取り付けられている場合は、取り外してください。また、取り外したケーブルキャップは大切に保管しておいてください。

- 接続するコネクタを確認してください。マザーボード上の「SATA1」コネクタに接続したケーブルはディスクベイ1に取り付けたハードディスクへ、「SATA2」コネクタに接続したケーブルはディスクベイ2に取り付けたハードディスクドライブへ接続します。

- 電源ケーブルはインタフェースケーブルの下を通るようにケーブリングしてください。

11. 手順2と逆の手順で本体を組み立てる。
12. BIOSセットアップユーティリティを起動して、BIOSからハードディスクドライブが正しく認識されていることを確認する(336ページ)。
13. 「システムBIOSのセットアップ」を参照してSATA RAIDの設定を有効にする。
14. 5章の「ディスクアレイコンフィグレーション」を参照してRAID1のディスクアレイドライブを作成する。
15. システムの再セットアップをする。

    詳しくは3章を参照してください。
16. バックアップをとっていたデータをリストアする。

    バックアップをとっていた場合はリストアしてください。詳しくは3章を参照してください。

取り外し

次に示す手順でハードディスクドライブを取り外します。

重要

- ハードディスクドライブ内のデータについて

  取り外したハードディスクドライブに保存されている大切なデータ(例えば顧客情報や企業の経理情報など)が第三者へ漏洩することのないようにお客様の責任において確実に処分してください。

  オペレーティングシステムのコマンドを使って削除しても、見た目は消去されたように見えますが、実際のデータはハードディスクドライブに書き込まれたままの状態にあります。完全に消去されていないデータは、特殊なソフトウェアにより復元され、予期せぬ用途に転用されるおそれがあります。

  このようなトラブルを回避するために市販の消去用ソフトウェア(有償)またはサービス(有償)を利用し、確実にデータを処分することを強くお勧めします。データの消去についての詳細は、お買い求めの販売店または保守サービス会社にお問い合わせください。

- 電源ケーブルを取り外すときは、次の注意を守ってください。

  - ケーブルをねじらない。
  - ケーブル部分を持って引っ張らない。
  - コネクタ部分を持ってまっすぐに引き抜く。

- ディスクベイ2に取り付けていたハードディスクドライブを取り外したまま使用する場合は、接続していた電源ケーブルのコネクタにケーブルキャップをつけてください。ケーブルキャップは出荷時に電源ケーブルに取り付けられていたものです(または付属品として添付されている場合もあります)。

1. 336ページを参照して準備をする。
2. ハードディスクドライブに接続しているケーブルをすべて取り外す。
3. 「取り付け」の手順4～7を参照してディスクベイを取り外す。
4. 「取り付け」の手順8、9を参照してハードディスクドライブを取り外す。
5. ハードディスクを交換する場合は、ハードディスクドライブをディスクベイに取り付ける。
6. 「取り付け」の手順10を参照してディスクベイを取り付け、ケーブルを接続する。
7. 手順1と逆の手順で本体を組み立てる。
8. ディスクアレイを構築している場合はリビルドなどの必要な作業を行う。

   詳しくは397ページを参照してください。

DIMM

DIMM(Dual Inline Memory Module)は、本体のマザーボード上のDIMMソケットに取り付けます。

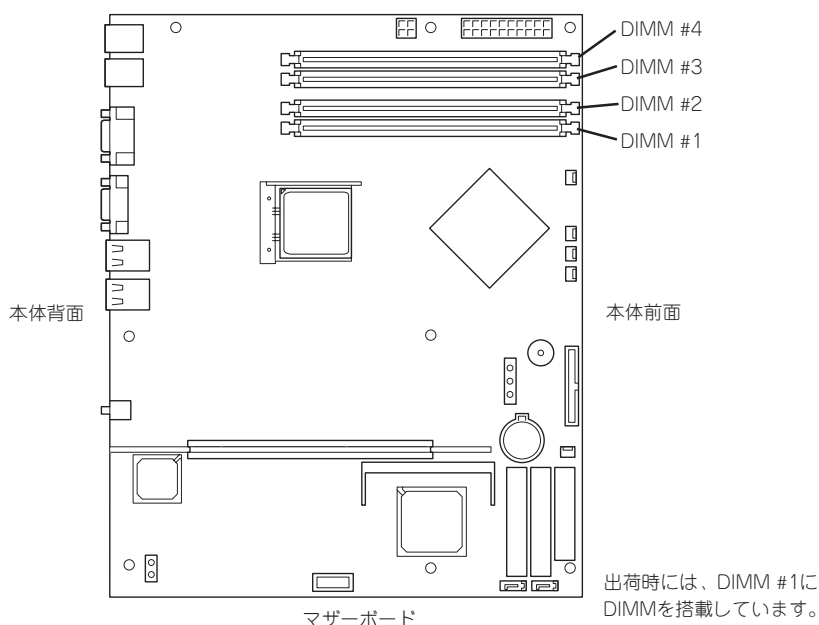
マザーボード上にはDIMMを取り付けるソケットが4個あります。

メモリは最大4GBまで増設できます。

重要

- **DIMMは大変静電気に弱い電子部品です。本体の金属フレーム部分などに触れて身体の静電気を逃がしてからDIMMを取り扱ってください。また、ボードの端子部分や部品を素手で触ったり、DIMMを直接机の上に置いたりしないでください。静電気に関する説明は335ページで詳しく説明しています。**
- **弊社で指定していないDIMMを使用しないでください。サードパーティのDIMMなどを取り付けると、DIMMだけでなく本体が故障するおそれがあります。また、これらの製品が原因となった故障や破損についての修理は保証期間中でも有料となります。**

また、本装置ではメモリのDual Channelメモリモードをサポートしています。

Dual Channelメモリモードで動作させるとメモリのデータ転送速度が2倍となります。

DIMMの増設順序

DIMMは、Dual Channelメモリモードを使用する場合と使用しない場合で増設順序や増設単位が異なります。

- **Dual Channelメモリモードを使用しない場合**

  増設単位および増設順序に制限はありません。

- **Dual Channelメモリモードを使用する場合**

  次の条件を守ってください。

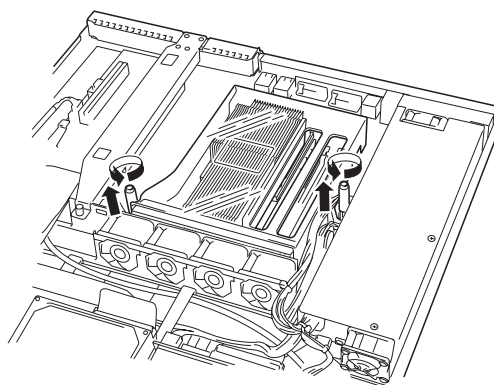
  - 2枚単位で取り付けてください。
  - 取り付ける2枚のメモリは同じ容量で同じ仕様のものを使ってください。
  - 取り付けるスロットはスロット1と3、または2と4を一組としてください(使用する組に順序はありません)。

  次に搭載例を示します。

搭載例	Dual Channel メモリモード	スロット1	スロット2	スロット3	スロット4
例1	動作する	256MB DIMM (標準)	(未搭載)	256MB DIMM	(未搭載)
例2	動作する	256MB DIMM (標準)	512MB DIMM	256MB DIMM	512MB DIMM
例3	動作しない	256MB DIMM (標準)	512MB DIMM	256MB DIMM	(未搭載)
例4	動作しない	256MB DIMM (標準)	512MB DIMM	(未搭載)	512MB DIMM

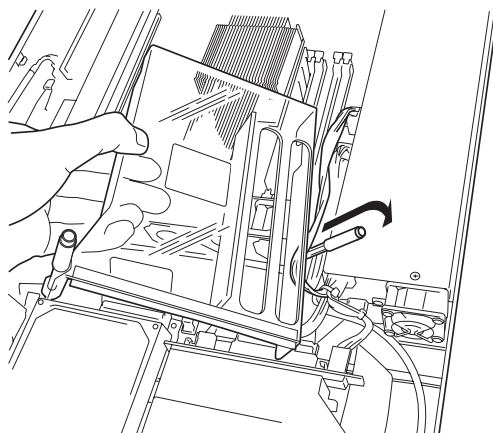
取り付け

次の手順に従ってDIMMを取り付けます。

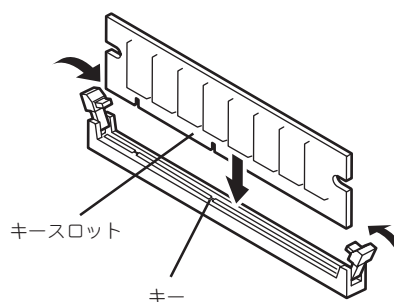
1. 336ページを参照して準備をする。
2. エアダクトの緑色のクリップ(2個)を持ち上げて反時計回りにまわしてネジをゆるめる。

重要

ドライバなどでネジを外す必要はありません。クリップを持ち上げて回すとネジは外れます。

3. エアダクトをまっすぐ持ち上げて取り外す。

チェック

ケーブルをひっかけていないことを確認してください。

4. 取り付けるDIMMソケットの両端にあるレバーを左右に広げ、DIMMをソケットにまっすぐ押し込む。

チェック

DIMMの向きに注意してください。DIMMの端子側には誤挿入を防止するための切り欠きがあります。

DIMMがDIMMソケットに差し込まれるとレバーが自動的に閉じます。

5. 手順1で取り外した部品を取り付ける。

チェック

エアダクトを取り付ける際に次の点を確認してください。

- マザーボード上のコネクタやピン、電子部品にぶつかっていないこと。
- 電源ユニット側にある電源ケーブルがエアダクトの上に配置されていないこと。

6. DianaScopeを使って管理PCから、本装置のBIOSセットアップユーティリティを起動して「Advanced」メニューの「Memory Configuration」で増設したDIMMがBIOSから認識されていること(画面に表示されていること)を確認する(367ページ参照)。

   「DianaScope」についてはEXPRESSBUILDER(SE) CD-ROM内のオンラインドキュメントを参照してください。

7. 「Advanced」メニューの「Reset Configuration Data」を「Yes」にする。

   ハードウェアの構成情報を更新するためです。詳しくは366ページをご覧ください。

8. BIOSセットアップユーティリティの設定を保存して終了する。

9. DianaScopeを終了する。

取り外し

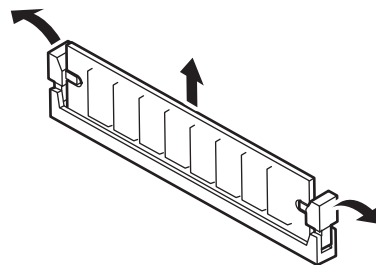
次の手順に従ってDIMMを取り外します。

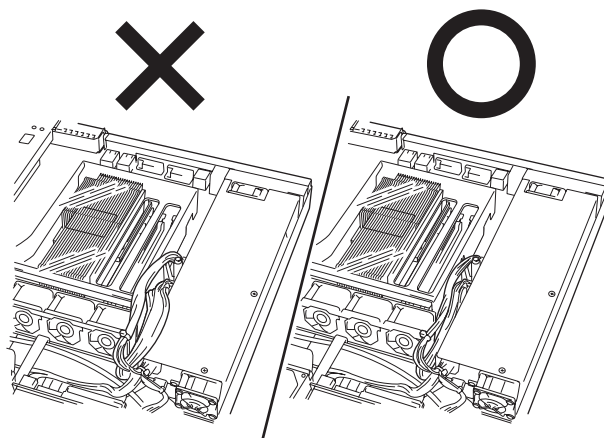
- 故障したDIMMを取り外す場合は、POSTやESMPROで表示されるエラーメッセージを確認して、取り付けているDIMMソケットを確認してください。
- DIMMは最低1枚搭載されていないと装置は動作しません。

1. 336ページを参照して準備をする。
2. エアダクトをまっすぐ持ち上げて取り外す。

ケーブルをひっかけていないことを確認してください。

3. 取り外すDIMMのソケットの両側にあるレバーを左右にひろげる。

   ロックが解除されDIMMを取り外せます。

4. 手順1と2で取り外した部品を取り付ける。

> チェック
>
> エアダクトを取り付ける際に次の点を確認してください。
>
> - マザーボード上のコネクタやピン、電子部品にぶつかっていないこと。
> - 電源ユニット側にある電源ケーブルがエアダクトの上に配置されていないこと。
>
>

5. DianaScopeを使って管理PCから、本装置のBIOSセットアップユーティリティを起動して「Advanced」メニューの「Memory Configuration」で増設したDIMMがBIOSから認識されていること(画面に表示されていること)を確認する(367ページ参照)。

   「DianaScope」についてはEXPRESSBUILDER(SE)CD-ROM内のオンラインドキュメントを参照してください。

6. 「Advanced」メニューの「Reset Configuration Data」を「Yes」にする。

   ハードウェアの構成情報を更新するためです。詳しくは366ページをご覧ください。

7. 故障したDIMMを交換した場合は、「Advanced」メニューの「Memory Configuration」で、「Memory Retest」を「Yes」にする。

   エラー情報をクリアするためです。詳しくは367ページをご覧ください。

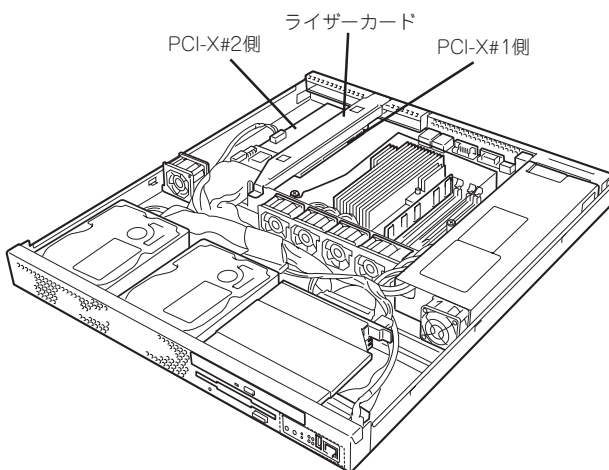
8. BIOSセットアップユーティリティの設定を保存して終了する。

9. DianaScopeを終了する。

PCIボード

本体のマザーボード上にはライザーカードが搭載されています。ライザーカードには、PCIボードを取り付けることのできるスロットが2個あります。

重要

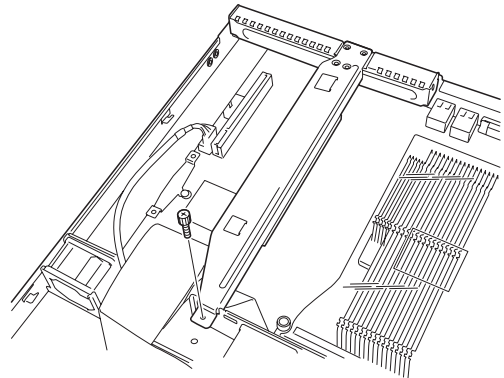
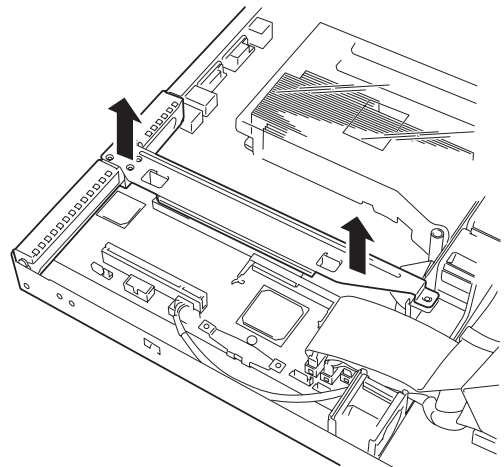
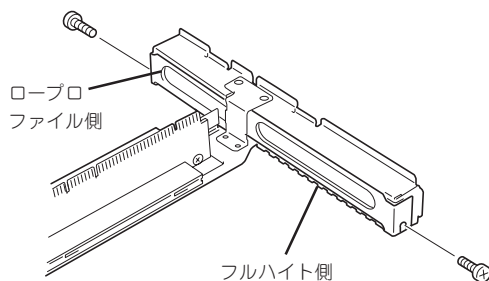
PCIボードやライザーカードは大変静電気に弱い電子部品です。本体の金属フレーム部分などに触れて身体の静電気を逃がしてからボードを取り扱ってください。また、PCIボードおよびライザーカードの端子部分やボードに実装されている部品の信号ピンに触れたり、PCIボードおよびライザカードを直接机の上に置いたりしないでください。静電気に関する説明は335ページで詳しく説明しています。

<table>
<tr><th rowspan="6">型名</th><th rowspan="6">部品名</th><th></th><th colspan="2">スロット（バスA）</th><th rowspan="6">備考</th></tr>
<tr><th></th><th>PCI-X#1</th><th>PCI-X#2</th></tr>
<tr><th>PCIスロット</th><th>64bit/66MHz</th><th>64bit/66MHz</th></tr>
<tr><th>スロットサイズ</th><th>Low Profile</th><th>Full Height</th></tr>
<tr><th>PCIボードタイプ</th><th>3.3V</th><th>3.3V</th></tr>
<tr><th>搭載可能なボードタイプ</th><th>MD2</th><th>ショート</th></tr>
<tr><td>N8104-88</td><td colspan="2">100BASE-TX接続ボード</td><td>○</td><td>−</td><td></td></tr>
<tr><td>N8104-113</td><td colspan="2">1000BASE-T接続ボード(2ch)</td><td>−</td><td>○</td><td>同等品を標準で実装済み。</td></tr>
<tr><td>N8104-109</td><td colspan="2">1000BASE-SX接続ボード</td><td>○</td><td>−</td><td></td></tr>
<tr><td>N8104-115</td><td colspan="2">1000BASE-T接続ボード</td><td>○</td><td>−</td><td></td></tr>
</table>

取り付け

次の手順に従ってPCIボードスロットにボードを取り付けます。

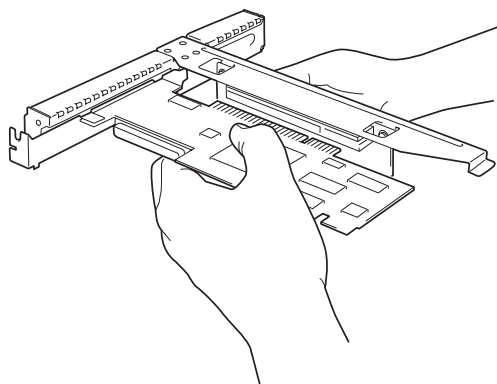
PCIボードを取り付けるときは、ボードの接続部の形状とPCIボードスロットのコネクタ形状が合っていることを確認してください。

本装置に取り付けることのできるPCIボードはショートタイプのみです。ロングタイプは取り付けることができません。

1. 336ページを参照して準備をする。
2. ライザーカードを固定しているネジ1本を外す。

3. ライザーカードの両端を持ってまっすぐ持ち上げて本体から取り外す。

4. ライザーカードからネジ1本を外し、増設スロットカバーを取り外す。

重要

取り外した増設スロットカバーは、大切に保管しておいてください。

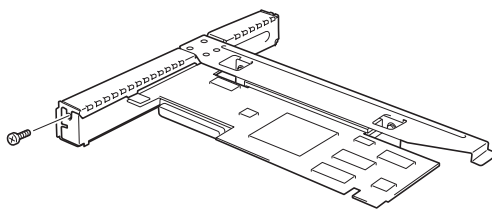
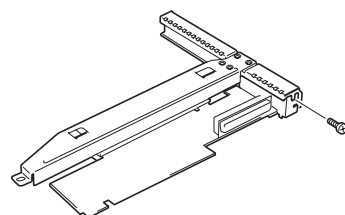
5. ライザーカードにPCIボードを取り付ける。

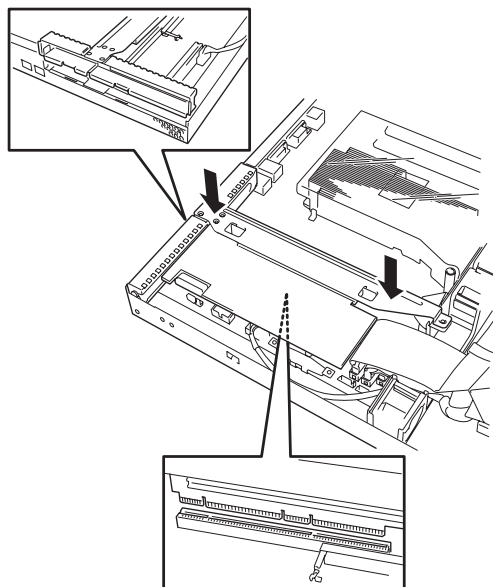
   ライザーカードのスロット部分とPCIボードの端子部分を合わせて、確実に差し込みます。

重要

- **ライザーカードやPCIボードの端子部分およびボードに実装されている電子部品の信号ピンには触れないでください。汚れや油が付いた状態で取り付けると誤動作の原因となります。**
- **うまくボードを取り付けられないときは、ボードをいったん取り外してから取り付け直してください。ボードに過度の力を加えるとPCIボードやライザーカードを破損するおそれがありますので注意してください。**

チェック

PCIボードのブラケットの端が、ライザーカードのフレーム穴に差し込まれていることを確認してください。

6. PCIボードを手順3で外したネジで固定する。

7. ライザーカードをマザーボードのスロットに接続する。

   ライザーカードの端子部分とマザーボード上のスロット部分を合わせて、確実に差し込みます。

チェック

差し込む際にライザーカードのフレームにある、筐体フレームに引っかけるためのツメが正しく勘合していることを確認してください。また、差し込んだ後、図のようにライザーカードのフレームを指で押し、ライザーカードの端子部分が完全に見えなくなるまで押し込んでください。

8. 取り外した部品を取り付ける。

9. DianaScopeを使って本装置のBIOSセットアップユーティリティを起動して、「Advanced」メニューの「Reset Configuration Data」を「Yes」にする。

   ハードウェアの構成情報を更新するためです。詳しくは366ページをご覧ください。また、必要に応じて搭載したボードが持つオプションROMの展開をするかどうかを確認してください。

   DianaScopeについてはEXPRESSBUILDER(SE)CD-ROM内のオンラインドキュメントを参照してください。

取り外し

ボードの取り外しは、取り付けの逆の手順を行ってください。
ボードをしっかりと持って取り外してください。また、取り外しの際に本体が動かないよう別の人に本体を押さえてもらいながら取り外しを行ってください。

PCIスロットに搭載したオプションのLANボードに接続したケーブルを抜くときは、コネクタのツメが手では押しにくくなっているため、マイナスドライバなどを使用してツメを押して抜いてください。その際に、マイナスドライバなどがLANポートやその他のポートを破損しないよう十分に注意してください。

ボードを取り外したまま運用する場合は、ライザーカードに取り付けられていた増設スロットカバーを必ず取り付けてください。増設スロットカバーはネジで固定してください。

ボードの取り外しや交換・取り付けスロットの変更をした場合は、DianaScopeを使って本装置のBIOSセットアップユーティリティを起動して、「Advanced」メニューの「Reset Configuration Data」を「Yes」にして、ハードウェアの構成情報を更新してください。

システムBIOSのセットアップ(SETUP)

Basic Input Output System(BIOS)の設定方法について説明します。

導入時やオプションの増設/取り外し時にはここで説明する内容をよく理解して、正しく設定してください。

概　要

SETUPはハードウェアの基本設定をするためのユーティリティツールです。このユーティリティは本体内のフラッシュメモリに標準でインストールされているため、専用のユーティリティなどがなくても実行できます。

SETUPで設定される内容は、出荷時に最も標準で最適な状態に設定していますのでほとんどの場合においてSETUPを使用する必要はありませんが、この後に説明するような場合など必要に応じて使用してください。

重要

- SETUPの操作は、システム管理者(アドミニストレータ)が行ってください。
- SETUPでは、パスワードを設定することができます。パスワードには、「Supervisor」と「User」の2つのレベルがあります。「Supervisor」レベルのパスワードでSETUPにアクセスした場合、すべての項目の変更ができます。「Supervisor」のパスワードが設定されている場合、「User」レベルのパスワードでは、設定内容を変更できる項目が限られます。
- OS(オペレーティングシステム)をインストールする前にパスワードを設定しないでください。
- SETUPユーティリティは、最新のバージョンがインストールされています。このため設定画面が本書で説明している内容と異なる場合があります。設定項目については、オンラインヘルプを参照するか、保守サービス会社に問い合わせてください。

起　動

起動と操作には「DianaScope」をインストールしたコンピュータ（管理PC）が必要です。詳しくはEXPRESSBUILDER（SE） CD-ROM内のオンラインドキュメントを参照してください。
本体の電源をONにすると管理PCのディスプレイ装置の画面にPOST（Power On Self-Test）の実行内容が表示されます。「NEC」ロゴが表示された場合は、<Esc>キーを押してください。

しばらくすると、次のメッセージが画面左下に表示されます。

```
Press <F2> to enter SETUP or Press <F12> to boot from Network
```

ここで<F2>キーを押すと、SETUPが起動してMainメニュー画面を表示します。

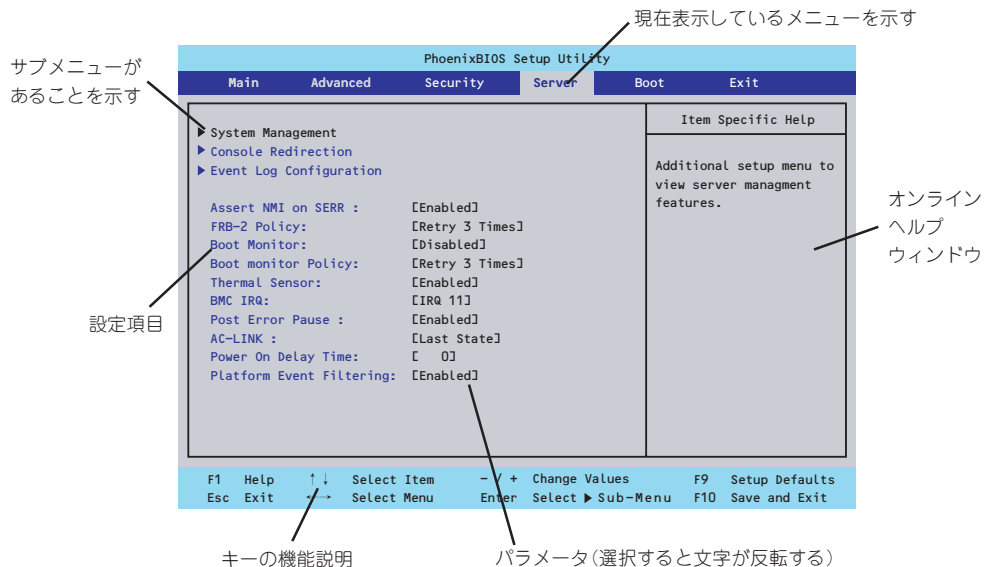
以前にSETUPを起動してパスワードを設定している場合は、パスワードを入力する画面が表示されます。パスワードを入力してください。

```
Enter password:[                        ]
```

パスワードの入力は、3回まで行えます。3回とも誤ったパスワードを入力すると、本装置は動作を停止します（これより先の操作を行えません）。電源をOFFにしてください。

パスワードには、「Supervisor」と「User」の2種類のパスワードがあります。「Superoisor」では、SETUPでのすべての設定の状態を確認したり、それらを変更したりすることができます。「User」では、確認できる設定や、変更できる設定に制限があります。

キーと画面の説明

管理PCのキーボード上の次のキーを使ってSETUPを操作します(キーの機能については、画面下にも表示されています)。

□ カーソルキー(↑、↓)
画面に表示されている項目を選択します。文字の表示が反転している項目が現在選択されています。

□ カーソルキー(←、→)
MainやAdvanced、Security、Server、Boot、Exitなどのメニューを選択します。

□ <−>キー/<+>キー
選択している項目の値(パラメータ)を変更します。サブメニュー(項目の前に「▶」がついているもの)を選択している場合、このキーは無効です。

□ <Enter>キー
選択したパラメータの決定を行うときに押します。

□ <Esc>キー
ひとつ前の画面に戻ります。押し続けると「Exit」メニューに進みます。

□ <F1>キー
SETUPの操作でわからないことがあったときはこのキーを押してください。SETUPの操作についてのヘルプ画面が表示されます。<Esc>キーを押すと、元の画面に戻ります。

□ <F9>キー
現在表示している項目のパラメータをデフォルトのパラメータに戻します(出荷時のパラメータと異なる場合があります)。

□ <F10>キー
設定したパラメータを保存してSETUPを終了します。

設定例

次にソフトウェアと連携した機能や、システムとして運用するときに必要となる機能の設定例を示します。

日付・時間の設定

日付や時間の設定は、オペレーティングシステム上でもできます。
「Main」→「System Time」(時刻の設定)
「Main」→「System Date」(日付の設定)

管理ソフトウェアとの連携関連

「ESMPRO/ServerManager」を使ってネットワーク経由で本体の電源を制御する
「Advanced」→「Advanced Chipset Control」→「Wake On LAN/PME」→「Enabled」
「Server」→「AC-LINK」→「StayOff」

ハードディスクドライブ関連

ハードディスクドライブの状態を確認する
「Main」→「Serial ATA Channel 0 Master/Serial ATA Channel 1 Master」→表示を確認する

シリアルATAハードディスクドライブでRAIDを組む
「Advanced」→「SATARAID Enable」→「Enable」→再起動後、RAIDのコンフィグレーションをする(387ページ参照)

「Load Setup Default」やCMOSクリアを行った場合は必ず、「Enabled」に設定を戻してください。初期値(「Disabled」)のまま起動するとハードディスクドライブのデータが壊れる場合があります。

UPS関連

UPSと電源連動させる

- UPSから電源が供給されたら常に電源をONさせる

  「Server」→「AC-LINK」→「Power On」

- UPSから電源が供給されても電源をOFFのままにする

  「Server」→「AC-LINK」→「StayOff」

起動関連

本体に接続している起動デバイスの順番を変える

「Boot」→起動順序を設定する

POSTの実行内容を表示する

「Advanced」→「Boot-time Diagnostic Screen」→「Enabled」

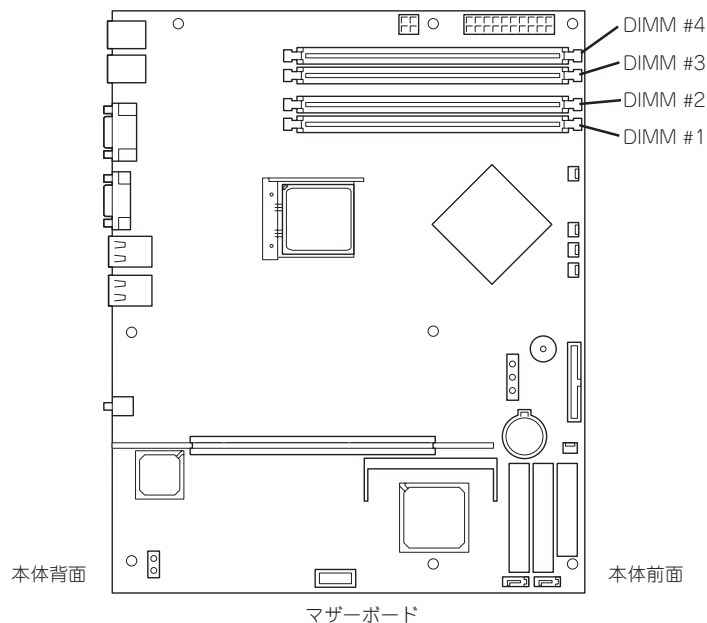
コンソール端末から制御する

「Server」→「Console Redirection」→それぞれの設定をする

メモリ関連

搭載しているメモリ(DIMM)の状態を確認する

「Advanced」→「Memory Configuration」→表示を確認する

画面に表示されているDIMMグループとマザーボード上のソケットの位置は下図のように対応しています。

メモリ(DIMM)のエラー情報をクリアする

「Advanced」→「Memory Configuration」→「Memory Retest」→「Yes」→<Enter>キー→再起動するとクリアされる

メモリ(DIMM)の詳細テストを実行する

「Advanced」→「Memory Configuration」→「Extended RAM Step」→「1MB」→再起動すると詳細テストを実行する

CPU関連

搭載しているCPUの状態を確認する

「Main」→「Processor Settings」→「Processor 1 CPUID」→表示を確認する

CPUのエラー情報をクリアする

「Main」→「Processor Settings」→「Processor Retest」→「Yes」→再起動するとクリアされる

キーボード関連

Numlockを設定する

「Advanced」→「NumLock」→「Off(起動時に無効)/On(起動時に有効)」

イベントログ関連

イベントログをクリアする

「Server」→「Event Log Configuration」→「Clear All Event Logs」→<Enter>キー→再起動するとクリアされる

セキュリティ関連

BIOSレベルでのパスワードを設定する

「Security」→「Set Supervisor Password」→パスワードを入力する
「Security」→「Set User Password」→パスワードを入力する
管理者パスワード(Supervisor)、ユーザーパスワード(User)の順に設定します。

外付け周辺機器関連

外付け周辺機器に対する設定をする

「Advanced」→「Peripheral Configuration」→それぞれの機器に対して設定をする

内蔵機器関連

本体内蔵のコントローラに対する設定をする

「Advanced」→「Advanced Chipset Control」→「PCI Device」→それぞれのデバイスに対して設定をする

取り付けたオプションのPCIボードのROM展開を有効にする。

「Advanced」→「PCI Configuration」→「PCI Slot n Option ROM(n:スロット番号)」→「Enabled」

ハードウェアの構成情報をクリアする(内蔵機器の取り付け/取り外しの後)

「Advanced」→「Reset Configuration Data」→「Yes」

設定内容のセーブ関連

本体標準装備のHostRAIDを使用してシリアルATAハードディスクドライブをディスクアレイで使用している場合は必ず、「Advanced」メニューの「SATA RAID Enable」を「Enabled」に設定してください。初期値(「Disabled」)のまま起動するとハードディスクドライブのデータが壊れる場合があります。

BIOSの設定内容を保存して終了する

「Exit」→「Exit Saving Changes」

変更したBIOSの設定を破棄して終了

「Exit」→「Exit Discarding Changes」

BIOSの設定をデフォルトの設定に戻す

「Exit」→「Load Setup Defaults」

変更したBIOSの設定を破棄する

「Exit」→「Discard Changes」

現在の設定内容を保存する

「Exit」→「Save Changes」

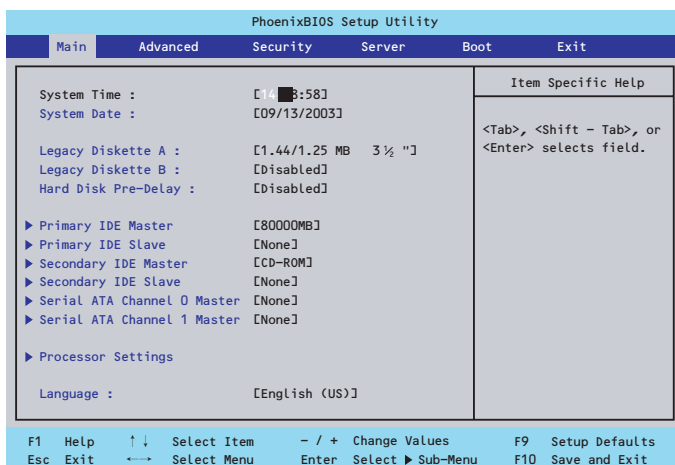
パラメータと説明

SETUPには大きく6種類のメニューがあります。

- Mainメニュー
- Advancedメニュー
- Securityメニュー
- Serverメニュー
- Bootメニュー
- Exitメニュー

このメニューの中からサブメニューを選択することによって、さらに詳細な機能の設定ができます。次に画面に表示されるメニュー別に設定できる機能やパラメータ、出荷時の設定を説明をします。

Main

SETUPを起動すると、はじめにMainメニューが表示されます。項目の前に「▶」がついているメニューは、選択して<Enter>キーを押すとサブメニューが表示されます。

Mainメニューの画面上で設定できる項目とその機能を示します。

項　目	パラメータ	説　明
System Time	HH:MM:SS	時刻の設定をします。
System Date	MM/DD/YYYY	日付の設定をします。
Legacy Diskette A	Disabled 360 Kb　5 1/4 1.2 MB　5 1/4 720 Kb　3 1/2 [1.44/1.25MB 31/2] 2.88 MB　3 1/2	フロッピーディスクドライブ（標準装備）の設定をします。
Legacy Diskette B	[Disabled] 360 Kb　5 1/4 1.2 MB　5 1/4 720 Kb　3 1/2 1.44/1.25MB 31/2 2.88 MB　3 1/2	本装置には2台目のフロッピーディスクドライブはありません。出荷時の設定のままにしておいてください。
Hard Disk Pre-Delay	[Disabled] 3 Seconds 6 Seconds 9 Seconds 12 Seconds 15 Seconds 21 Seconds 30 Seconds	POST中に初めて内蔵のIDEハードディスクドライブにアクセスする際にハードディスクドライブの準備のための待ち時間を設定します。
Primary IDE Master Primary IDE Slave Secondary IDE Master Secondary IDE Slave Serial ATA Channel 0 Master Serial ATA Channel 1 Master	―	それぞれのチャネルに接続されているデバイスのタイプを表示します。 シリアルATAに接続されたデバイスの情報はPrimary IDEのエリアに表示されます。 一部設定を変更できる項目がありますが、出荷時の設定のままにしておいてください。
Processor Settings	―	サブメニューを表示します。次ページを参照してください。
Language	[English(US)] Francais Deutsch Espanol Italiano	SETUPで表示する言語を選択します。

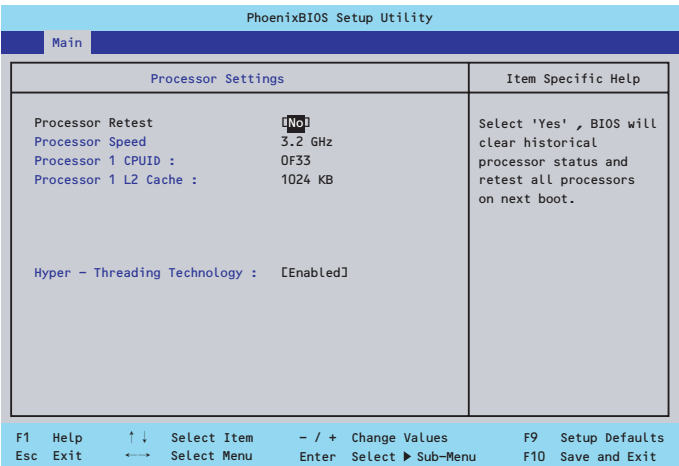
[　]: 出荷時の設定

BIOSのパラメータで時刻や日付の設定が正しく設定されているか必ず確認してください。次の条件に当てはまる場合は、運用の前にシステム時計の確認・調整をしてください。

- **装置の輸送後**
- **装置の保管後**
- **装置の動作を保証する環境条件(温度：10℃～35℃・湿度：20%～80%)から外れた条件下で休止状態にした後**

システム時計は毎月1回程度の割合で確認してください。また、高い時刻の精度を要求するようなシステムに組み込む場合は、タイムサーバ(NTPサーバ)などを利用して運用することをお勧めします。
システム時計を調整しても時間の経過と共に著しい遅れや進みが生じる場合は、お買い求めの販売店、または保守サービス会社に保守を依頼してください。

Processor Settings

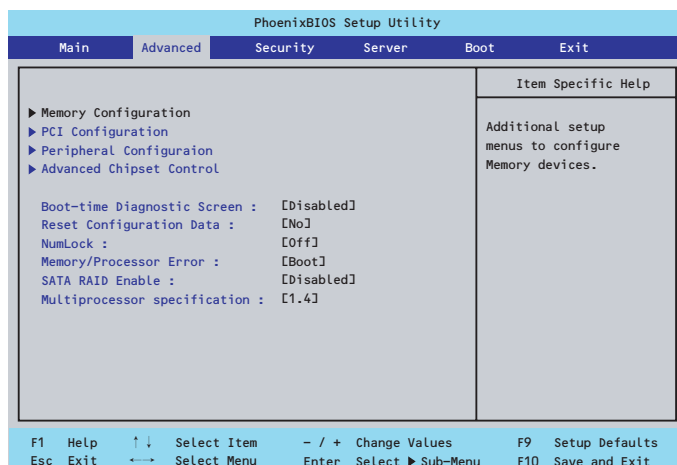
Mainメニューで「Processor Settings」を選択すると、以下の画面が表示されます。

項目については次の表を参照してください。

項　目	パラメータ	説　明
Processor Retest	[No] Yes	プロセッサのエラー情報をクリアし、次回起動時にすべてのプロセッサに対してテストを行います。このオプションは次回起動時に自動的に「No」に切り替わります。
Processor Speed	nnn GHz	プロセッサの動作周波数を表示します（表示のみ）。
Processor 1 CPUID	数値(0Fxx) Disabled	数値の場合はプロセッサのIDを示します。「Disabled」はプロセッサの故障を示します（表示のみ）。
Processor 1 L2 Cache	nnn KB	プロセッサの二次キャッシュサイズを表示します（表示のみ）。
Hyper-Threading Technology	[Enabled] Disabled	1つの物理CPUを2つの論理CPUとしてみせて動作させる機能です。Enabledに設定すると1つのCPUが2つに見えます。 注：Hyper-threading Technologyは、Hyper-threading Technologyに対応したCPUを搭載した場合のみ表示されます。

[　]: 出荷時の設定

Advanced

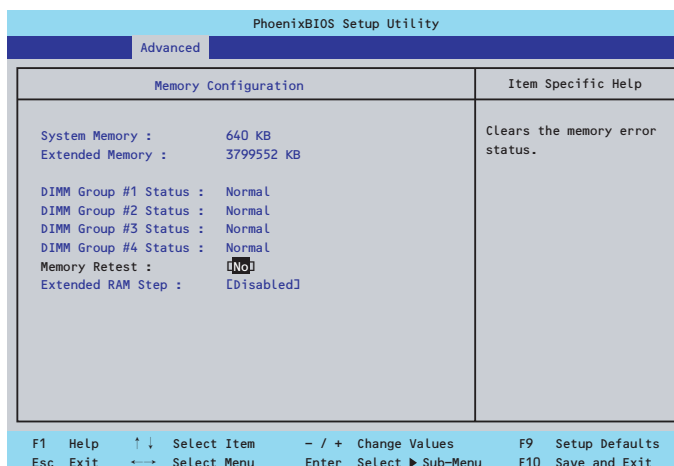
カーソルを「Advanced」の位置に移動させると、Advancedメニューが表示されます。

項目の前に「▶」がついているメニューは、選択して<Enter>キーを押すとサブメニューが表示されます。

項目については次の表を参照してください。

項　目	パラメータ	説　明
Boot-time Diagnostic Screen	Enabled [Disabled]	起動時の自己診断（POST）の実行画面を表示させるか、表示させないかを設定します。「Disabled」に設定すると、POSTの間、「NEC」ロゴが表示されます。（ここで<Esc>キーを押すとPOSTの実行画面に切り替わります。）
Reset Configuration Data	[No] Yes	Configuration Data(POSTで記憶しているシステム情報）をクリアするときは「Yes」に設定します。システムの起動後にこのパラメータは「No」に切り替わります。
NumLock	[Off] On	システム起動時にNumlockの有効/無効を設定します。
Memory/Processor Error	[Boot] Halt	POST中にメモリやCPUのエラーを検出したときにPOSTを中断するかどうかを設定します。
SATA RAID Enable	[Disabled] Enabled	オンボード上のSATAインタフェースを使ったハードディスクドライブのRAID（ディスクアレイ）の有効/無効を設定します。本装置ではハードディスクドライブを増設する場合は、必ず「Enabled」に設定を変更する必要があります。 注：異なる設定でSATAハードディスクドライブから起動するとデータが壊れるおそれがあります。
Multiprocessor Specification	[1.4] 1.1	マルチプロセッサ仕様で対応するバージョンを選択します。

[　]: 出荷時の設定

Memory Configuration

Advancedメニューで「Memory Configuration」を選択すると、以下の画面が表示されます。

項目については次の表を参照してください。

項　目	パラメータ	説　明
System Memory	—	本体内蔵の基本メモリ容量を表示します（表示のみ）。
Extended Memory	—	本体に内蔵された拡張メモリの総容量を表示します（表示のみ）。
DIMM Group #1 - #4 Status	Normal Not Installed Disabled	DIMMの状態を表示します（表示のみ）。「Normal」はDIMMが取り付けられていて、正常であることを、「Not Installed」はDIMMが取り付けられていていないことを示します。「Disabled」はDIMMが故障していることを示します。
Memory Retest	[No] Yes	メモリ(DIMM)の詳細テストを実行するかどうかを設定します。
Extended RAM Step	1MB [Disabled]	拡張メモリに対するテストを実行するかどうか、および実行する際のブロックサイズを設定します。

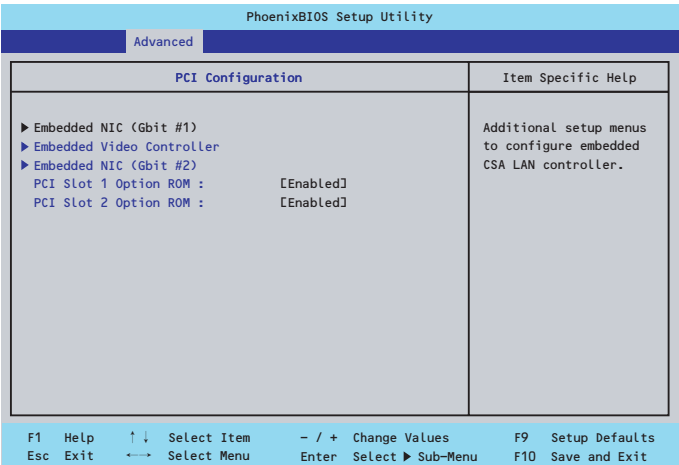
［　］: 出荷時の設定

PCI Configuration

Advancedメニューで「PCI Configuration」を選択すると、以下の画面が表示されます。項目の前に「▶」がついているメニューは、選択して<Enter>キーを押すとサブメニューが表示されます。

```
PhoenixBIOS Setup Utility
Advanced
PCI Configuration                              Item Specific Help

▶ Embedded NIC (Gbit #1)                       Additional setup menus
▶ Embedded Video Controller                    to configure embedded
▶ Embedded NIC (Gbit #2)                       CSA LAN controller.
  PCI Slot 1 Option ROM :        [Enabled]
  PCI Slot 2 Option ROM :        [Enabled]

F1   Help   ↑↓  Select Item   -/+    Change Values       F9   Setup Defaults
Esc  Exit   ←→  Select Menu   Enter  Select ▶ Sub-Menu   F10  Save and Exit
```

項　目	パラメータ	説　明
PCI Slot 1 Option POM PCI Slot 2 Option POM	[Enabled] Disabled	PCIスロットに接続されているデバイス（ボード）に搭載されているBIOSの有効/無効を設定するサブメニューを表示します。オプションROM BIOSを搭載したLANコントローラボードを使用していて、このボードからネットワークブートをしないときは「Disabled」にしてください。オプションROMの展開を無効にすることにより、メモリの消費を防ぎ、起動時間を短縮させることができます。

[　]: 出荷時の設定

Embedded NIC (Gbit #1)

項　目	パラメータ	説　明
Onboard CSA LAN Control	[Enabled] Disabled	オンボード上のLANコントローラの有効/無効を設定します。
Option ROM Scan	[Enabled] Disabled	オンボード上のLANコントローラのBIOSの展開の有効/無効を設定するサブメニューを表示します。

[　]: 出荷時の設定

Embedded Video Controller

項　目	パラメータ	説　明
Onboard VGA Control	[Enabled] Disabled	オンボード上のグラフィックスコントローラの有効/無効を設定します。

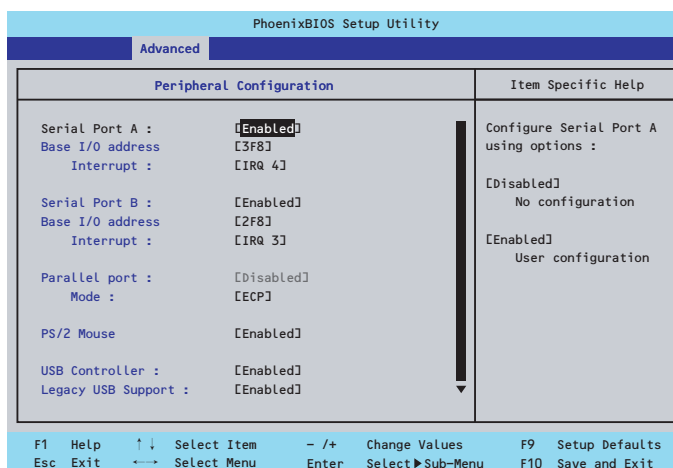
[　]: 出荷時の設定

Embedded NIC (Gbit #2)

項　目	パラメータ	説　明
Onboard KENAI Control	[Enabled] Disabled	オンボード上のKENAI LANコントローラの有効/無効を設定します。
Option ROM Scan	[Enabled] Disabled	オンボード上のネットワークコントローラのBIOSの展開の有効/無効を設定するサブメニューを表示します。

[　]: 出荷時の設定

Peripheral Configuration

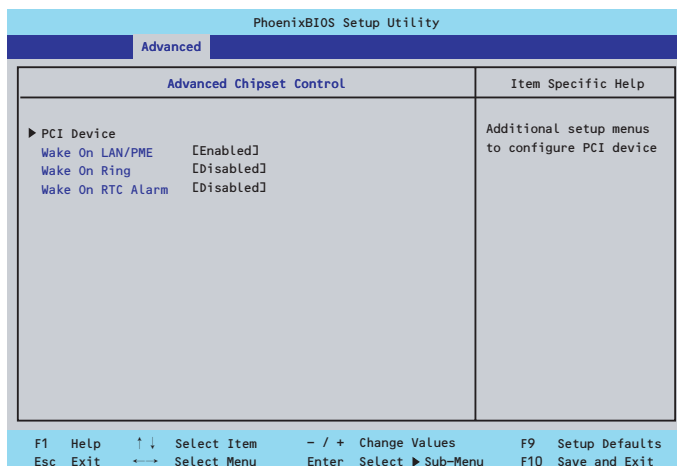
Advancedメニューで「Peripheral Configuration」を選択すると、以下の画面が表示されます。

項目については次の表を参照してください。

割り込みやベースI/Oアドレスが他と重複しないように注意してください。設定した値が他のリソースで使用されている場合は黄色の「＊」が表示されます。黄色の「＊」が表示されている項目は設定し直してください。

項　目	パラメータ	説　明
Serial Port A	Disabled [Enabled]	シリアルポートAを使用するかどうかを指定します。
Base I/O Adress	[3F8] 2F8 3E8 2E8	シリアルポートAに割り当てるI/Oアドレスを指定します。
Interrupt	IRQ 3 [IRQ 4]	シリアルポートAに割り当てる割り込みを指定します。
Serial Port B	Disabled [Enabled]	シリアルポートBを使用するかどうかを指定します。
Base I/O Adress	3F8 [2F8] 3E8 2E8	シリアルポートBに割り当てるI/Oアドレスを指定します。
Interrupt	[IRQ 3] IRQ 4	シリアルポートBに割り当てる割り込みを指定します。
Parallel Port	Disabled	パラレルポートを使用するかどうかを指定します。本装置では機能しません。
Mode	ー	パラレルポートに割り当てるモードを指定します。本装置では機能しません。
PS/2 Mouse	Disabled [Enabled]	PS/2マウスの有効/無効を設定します。
USB Controller	Disabled [Enabled]	USB機器の有効/無効を設定します。
Legacy USB Support	Disabled [Enabled]	USBを正式にサポートしていないOSでもUSBキーボードが使用できるようにするかどうかを設定します。
Serial ATA	Disabled [Enabled]	シリアルATAの有効/無効を設定します。

[　]: 出荷時の設定

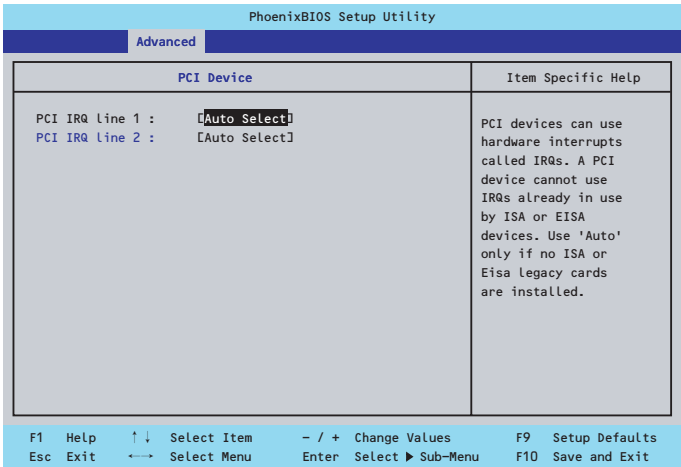
Advanced Chipset Control

Advancedメニューで「Advanced Chipset Control」を選択すると、以下の画面が表示されます。項目の前に「▶」がついているメニューは、選択して<Enter>キーを押すとサブメニューが表示されます。

項目については次の表を参照してください。

項　目	パラメータ	説　明
Wake On LAN/PME	Disabled [Enabled]	ネットワークを介したリモートパワーオン機能の有効/無効を設定します。
Wake On Ring	[Disabled] Enabled	シリアルポートを介したリモートパワーオン機能の有効/無効を設定します。
Wake On RTC Alarm	[Disabled] Enabled	リアルタイムクロックを利用したスケジューリングパワーオン機能の有効/無効を設定します。

[　]: 出荷時の設定

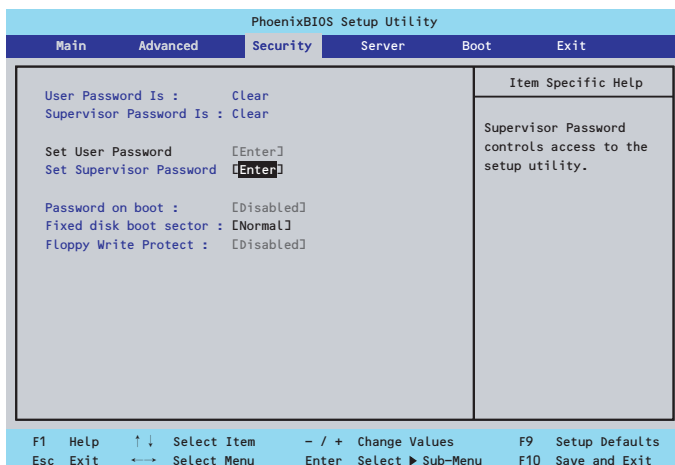
PCI Device

Advancedメニューの「Advanced Chipset Control」で「PCI Device」を選択すると、以下の画面が表示されます。

項目については次の表を参照してください。

項　目	パラメータ	説　明
PCI IRQ line 1～2	Disabled [Auto Select] IRQ 3 IRQ 4 IRQ 5 IRQ 6 IRQ 7 IRQ 9 IRQ 10 IRQ 11 IRQ 12 IRQ 14 IRQ 15	PCIバスにある2本の割り込み信号をどのIRQリクエストに割り当てるかを設定します。

[　]: 出荷時の設定

Security

カーソルを「Security」の位置に移動させると、Securityメニューが表示されます。

Set Supervisor PasswordもしくはSet User Passwordのどちらかで<Enter>キーを押すとパスワードの登録/変更画面が表示されます。
ここでパスワードの設定を行います。

重要

- **「User Password」は、「Supervisor Password」を設定していないと設定できません。**
- **OSのインストール前にパスワードを設定しないでください。**
- **パスワードを忘れてしまった場合は、「リセットとクリア」を参照して消去してください。**

各項目については次ページの表を参照してください。

項　目	パラメータ	説　明
User Password Is	Clear	パスワードの設定状態を示します。
Supervisor Password Is	Clear	パスワードの設定状態を示します。
Set User Password*	7文字までの英数字	<Enter>キーを押すとユーザーのパスワード入力画面になります。このパスワードではSETUPメニューへのアクセスが制限されます。
Set Supervisor Password	7文字までの英数字	<Enter>キーを押すとスーパーバイザのパスワード入力画面になります。このパスワードですべてのSETUPメニューにアクセスできます。この設定は、SETUPを起動したときのパスワードの入力で「Supervisor」でログオンしたときのみ設定できます。
Password on boot*	[Disabled] Enabled	起動時にパスワードの入力を行う/行わないの設定をします。先にスーパーバイザのパスワードを設定する必要があります。もし、スーパーバイザのパスワードが設定されていて、このオプションが無効の場合はBIOSはユーザーが起動していると判断します。
Fixed disk boot sector	[Normal] Write Protect	ハードディスクドライブのブートセクタへの書き込みを許可するか禁止するかどうかを設定します。
Floppy Write Protect	[Disabled] Enabled	フロッピーディスクドライブにセットしたフロッピーディスクへの書き込み権限を指定します。

* 「Set Supervisor Password」でパスワードを登録したときに指定できます。

[　]: 出荷時の設定

Server

カーソルを「Server」の位置に移動させると、Serverメニューが表示されます。
Serverメニューで設定できる項目とその機能を示します。項目の前に「▶」がついているメニューは、選択して<Enter>キーを押すとサブメニューが表示されます。

各項目については次の表を参照してください。

項　目	パラメータ	説　明
Assert NMI on SERR	Disabled [Enabled]	PCI SERRのサポートを設定します。
FRB-2 Policy	Disable FRB2 Timer [Retry 3 Times]	FRBレベル2のタイマに関する設定をします。
Boot Monitor	[Disabled] 5 Minutesから 60 Minutesの5分単位	起動監視機能の有効/無効とタイムアウトまでの時間を設定します。この機能を使用する場合は、ESMPRO/ServerAgentをインストールしてください。 ESMPRO/ServerAgentをインストールしていないOSから起動する場合には、この機能を無効にしてください。
Boot Monitor Policy	[Retry 3 Times] Retry Service Boot Always Reset	起動監視時にタイムアウトが発生した場合の処理を設定します。 [Retry 3 Times]に設定すると、タイムアウトの発生後にシステムをリセットし、OS起動を3回まで試行します。 [Retry Service Boot]に設定すると、タイムアウト発生後にシステムをリセットし、OS起動を3回まで試行します。その後、サービスパーティション*から起動を3回試み、3回とも失敗した場合は起動を停止します。 [Always Reset]に設定すると、タイムアウト発生後にOS起動を常に試みます。
Thermal Sensor	Disabled [Enabled]	温度センサ監視機能の有効/無効を設定します。有効にすると、温度の異常を検出した場合にPOSTの終わりでいったん停止します。
BMC IRQ	Disabled [IRQ 11]	BMC割り込みのIRQを設定します。

項　目	パラメータ	説　明
Post Error Pause	Disabled [Enabled]	POSTの実行中にエラーが発生した際に、POSTの終わりでPOSTをいったん停止するかどうか設定します。
AC-LINK	Stay Off [Last State] Power On	ACリンク機能を設定します。AC電源が再度供給されたときのシステムの電源の状態を設定します（下記参照）。
Power On Delay Time	[0] - 255	DC電源をONにするディレイ時間を0秒から255秒の間で設定します。AC-LINKで「Last State」または「Power On」に設定している場合に有効となります。
Platform Event Filtering	Disabled [Enabled]	リモートマネージメントカード（RMC）の通報機能が設定されている場合は、意味を持ちません。

[　]: 出荷時の設定

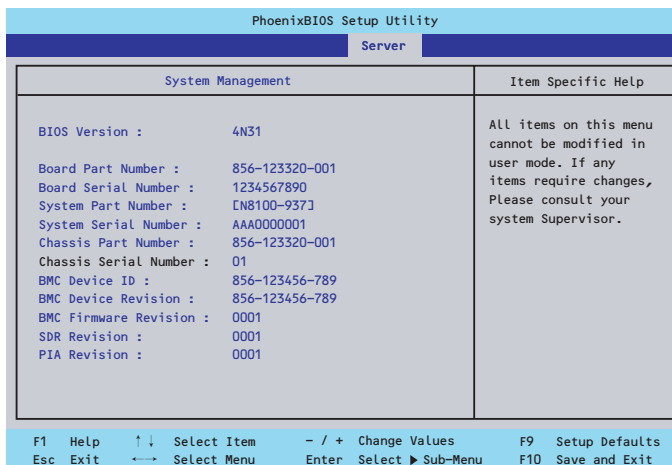
「AC-LINK」の設定と本体のAC電源がOFFになってから再度電源が供給されたときの動作を次の表に示します。

AC電源OFFの前の状態	設　定		
	Stay Off	Last State	Power On
動作中	Off	On	On
停止中（DC電源もOffのとき）	Off	Off	On
強制電源OFF*	Off	Off	On

* POWERスイッチを4秒以上押し続ける操作です。強制的に電源をOFFにします。

- 無停電電源装置（UPS）を接続する場合は、「Power On」に設定します。
- UPSに接続している場合も10秒以上経過してからONになるようにスケジューリングの設定をしてください。

System Management

Serverメニューで「System Management」を選択し、<Enter>キーを押すと、以下の画面が表示されます。

項目については次の表を参照してください。

項　目	パラメータ	説　明
BIOS Version	―	BIOSのバージョンを表示します（表示のみ）。
Board Part Number	―	マザーボードの部品番号を表示します（表示のみ）。
Board Serial Number	―	マザーボードのシリアル番号を表示します（表示のみ）。
System Part Number	―	本体のコードを表示します（表示のみ）。
System Serial Number	―	本体のシリアル番号を表示します（表示のみ）。
Chassis Part Number	―	シャーシの部品番号を表示します（表示のみ）。
Chassis Serial Number	―	シャーシのシリアル番号を表示します（表示のみ）。
BMC Device ID	―	BMC(Baseboard Management Controller)のデバイスIDを表示します（表示のみ）。
BMC Device Revision	―	BMC(Baseboard Management Controller）デバイスのレビジョンを表示します（表示のみ）。
BMC Firmware Revision	―	BMC(Baseboard Management Controller)ファームウェアのレビジョンを表示します（表示のみ）。
SDR Revision	―	SDR(Sensor Data Record)のレビジョンを表示します（表示のみ）。
PIA Revision	―	PIA(Platform Information Area)のレビジョンを表示します（表示のみ）。

Console Redirection

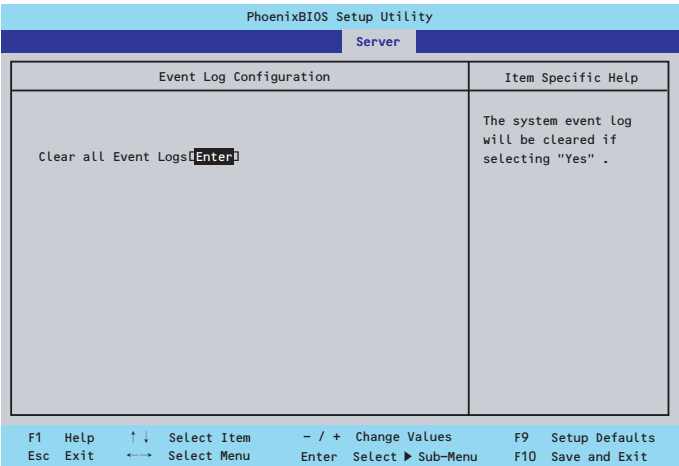
Serverメニューで「Console Redirection」を選択し、<Enter>キーを押すと、以下の画面が表示されます。

項目については次の表を参照してください。

項　目	パラメータ	説　明
BIOS Redirection Port	[Disabled] Serial Port A Serial Port B	コンソール端末が接続されているシリアルポートを設定します。
ACPI Redirection Port	[Disabled] Serial Port A Serial Port B	OS動作中に使用するコンソール端末が接続されているシリアルポートを設定します。
Baud Rate	9600 [19.2k] 38.4k 57.6k 115.2k	コンソール端末との通信速度（ボーレート）を設定します。
Flow Control	None XON/XOFF [CTS/RTS] CTS/RTS+CD	フロー制御の方法を設定します。
Terminal Type	[PC ANSI] VT 100+ VT-UTF8	ターミナル端末の種別を選択します。
Remote Console Reset	[Disabled] Enabled	コンソール端末からリセットコマンドの有効/無効を設定します。

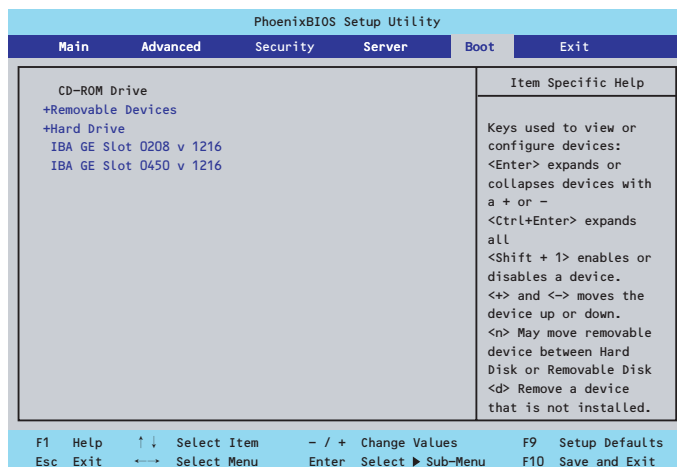
[　]: 出荷時の設定

EventLog Configuration

Serverメニューで「Event Log Configuration」を選択し、<Enter>キーを押すと、以下の画面が表示されます。

項目については次の表を参照してください。

項　目	パラメータ	説　明
Clear all Event Log	Enter	<Enter>キーを押すと確認画面が表示され、「Yes」を選ぶと保存されているエラーログを初期化します。

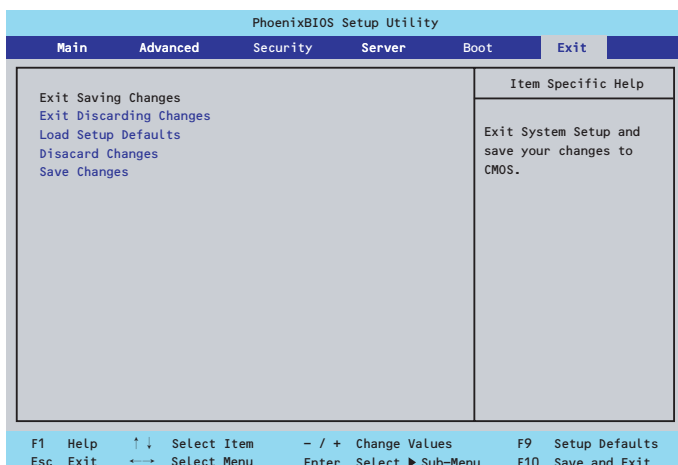
Boot

カーソルを「Boot」の位置に移動させると、起動順位を設定するBootメニューが表示されます。

システムは起動時にこのメニューで設定した順番に機器をサーチし、起動ソフトウェアを見つけるとそのソフトウェアで起動します。

<↑>キー/<↓>キー、<+>キー/<->キーで起動デバイスの優先順位を変更できます。
各機器の位置へ<↑>キー/<↓>キーで移動させ、<+>キー/<->キーで優先順位を変更できます。

EXPRESSBUILDER(SE)やバックアップCD-ROMを起動する場合は、上図に示す順番に設定してください。

Exit

カーソルを「Exit」の位置に移動させると、Exitメニューが表示されます。

このメニューの各オプションについて以下に説明します。

● Exit Saving Changes

新たに選択した内容をCMOSメモリ内に保存してSETUPを終わらせる時に、この項目を選択します。Exit Saving Changesを選択すると、確認の画面が表示されます。ここで、「Yes」を選ぶと新たに選択した内容をCMOSメモリ内に保存してSETUPを終了し、システムは自動的にシステムを再起動します。

● Exit Discarding Changes

新たに選択した内容をCMOSメモリ内に保存しないでSETUPを終わらせたい時にこの項目を選択します。ここで、「No」を選択すると、変更した内容を保存しないでSETUPを終わらせ、システムは自動的にシステムを再起動します。「Yes」を選択すると変更した内容をCMOSメモリ内に保存してSETUPを終了し、システムは自動的にシステムを再起動します。

● Load Setup Defaults

SETUPのすべての値をデフォルト値に戻したい時に、この項目を選択します。Load Setup Defaultsを選択すると、確認の画面が表示されます。ここで、「Yes」を選択すると、デフォルト値に戻ります。「No」を選択するとExitメニューの画面に戻ります。

このオプションを実行すると、「Advanced」メニューの「SATA RAID Enabled」が「Disabled」に設定されます。SATA内蔵ハードディスクドライブをディスクアレイで使用している場合は、SETUPを終了する前に「Enabled」に変更し、設定内容を保存してください。設定を変更せずに再起動するとハードディスクドライブのデータを壊すおそれがあります。

● Discard Changes

今まで変更した内容を破棄し、SETUPを起動する以前の設定に戻します。

● Save Changes

今まで変更した内容を保存し、SETUPを続けます。

リセットとクリア

本装置が動作しなくなったときやBIOSで設定した内容を出荷時の設定に戻すときに参照してください。

リセット

OSが起動する前に動作しなくなったときは、<Ctrl>キーと<Alt>キーを押しながら、<Delete>キーを押してください。リセットを実行します。

リセットは、本体のDIMM内のメモリや処理中のデータをすべてクリアしてしまいます。ハングアップしたとき以外でリセットを行うときは、本装置がなにも処理していないことを確認してください。

強制電源OFF

OSからシャットダウンできなくなったときや、POWERスイッチを押しても電源をOFFにできなくなったとき、リセットが機能しないときなどに使用します。

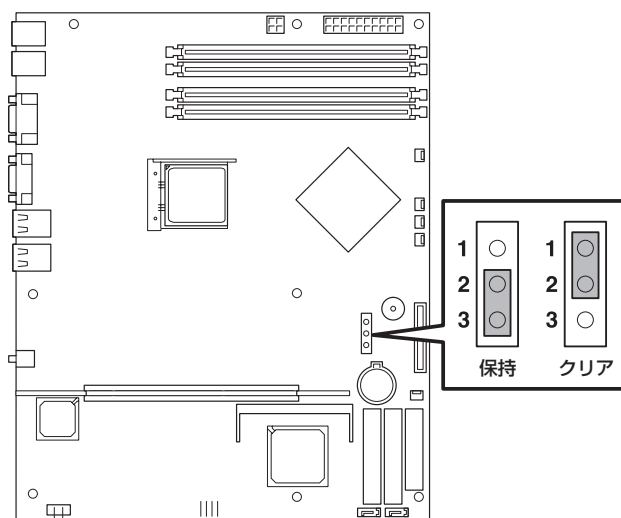
本体のPOWERスイッチを4秒ほど押し続けてください。電源が強制的にOFFになります。（電源を再びONにするときは、電源OFFから約10秒ほど待ってから電源をONにしてください。）

リモートパワーオン機能を使用している場合は、一度、電源をONにし直して、OSを起動させ、正常な方法で電源をOFFにしてください。

CMOSメモリ・パスワードのクリア

CMOSメモリに保存されている内容をクリアする場合は本体内部のコンフィグレーションジャンパスイッチを操作して行います。

重要

- CMOSメモリの内容をクリアするとBIOSセットアップユーティリティの設定内容がすべてデフォルトの設定に戻ります。
- その他のジャンパの設定は変更しないでください。装置の故障や誤動作の原因となります。
- CMOSメモリの内容をクリアすると、BIOS SETUPユーティリティの「Advanced」メニューの「SATA RAID Enabled」が「Disabled」に設定されます。SATA内蔵ハードディスクドライブをディスクアレイで使用している場合は、CMOSメモリのクリア後、BIOS SETUPユーティリティを起動して、上記設定を「Enabled」に変更し、設定内容を保存してください。設定を変更せずに起動するとハードディスクドライブのデータを壊すおそれがあります。

次にクリアする方法を示します。

装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 自分で分解・修理・改造はしない
- リチウムバッテリを取り外さない
- プラグを差し込んだまま取り扱わない

注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 中途半端に取り付けない
- カバーを外したまま取り付けない
- 高温注意
- 装置を引き出した状態にしない
- 指を挟まない
- 高温注意
- ラックが不安定な状態でデバイスをラックから引き出さない
- 複数台のデバイスをラックから引き出した状態にしない

本体内部の部品は大変静電気に弱い電子部品です。本体の金属フレーム部分などに触れて身体の静電気を逃がしてから取り扱ってください。内部の部品や部品の端子部分を素手で触らないでください。静電気に関する説明は155ページで詳しく説明しています。

1. 336ページを参照して準備をする。
2. ジャンパスイッチの設定を「保持」から「クリア」に変更する。

重要

- 本体のジャンパピン2-3に付いているクリップを使用してください。
- クリップをなくさないよう注意してください。

3. 3秒ほど待ってジャンパスイッチの設定を元に戻す。
4. 本体を元どおりに組み立ててPOWERスイッチを押す。
5. POST中に<F2>キーを押してBIOSセットアップユーティリティを起動して設定し直す。

SATA内蔵ハードディスクドライブをディスクアレイで使用している場合は、BIOS SETUPユーティリティの「Advanced」メニューの「SATA RAID Enabled」が「Enabled」になっていることを必ず確認してください。「Disabled」のまま起動するとハードディスクドライブのデータを壊すおそれがあります。

割り込みラインとI/Oポートアドレス

割り込みラインやI/Oポートアドレスは、出荷時に次のように割り当てられています。オプションを増設するときなどに参考にしてください。

- **割り込みライン**

出荷時では、次のように割り当てられています。

IRQ	周辺機器(コントローラ)	IRQ	周辺機器(コントローラ)
0	システムタイマ	8	リアルタイムクロック
1	キーボード	9	PCI
2	カスケード接続	10	PCI
3	COM Bシリアルポート	11	PCI/BMCIRQ
4	COM Aシリアルポート	12	マウス
5	PCI	13	数値演算プロセッサ
6	フロッピーディスク	14	プライマリIDE
7	PCI	15	セカンダリIDE

- **PIRQとPCIデバイスの関係**

出荷時では、Auto Detectに設定されています。PCIスロットにIRQを他のデバイスと共有できないボードを取り付けた場合は下表の設定例のように設定を変更してください。

メニュー項目	割り込み	IRQ設定例
PCI IRQ 1	LAN1	IRQ 7
PCI IRQ 2	LAN2	IRQ 7
PCI IRQ 3	—	Auto Select
PCI IRQ 4	USB Port 1/2	IRQ 5
PCI IRQ 5	PCIスロット#1	IRQ 10
PCI IRQ 6	—	Auto Select
PCI IRQ 7	—	Auto Select
PCI IRQ 8	USB Port 3	IRQ 5

● I/Oポートアドレス

アドレス*1	使用チップ*2
00-0F	DMA1コントローラ
20-21	割り込みコントローラ1
2E-2F	S-I/Oコンフィグレーション
40-43	タイマ1
4E-4F	(S-I/Oコンフィグレーション2)
60	キーボード/マウス
61	ノンマスカブルインターラプト
64	キーボード/マウス
70-73	リアルタイムクロック、ノンマスカブルインターラプト
80-8F	DMA1、DMA2
92	ポート92
A0-A1	割り込みコントローラ2
B2-B3	アドバンストパワーマネージメント
C0-D	FDMAコントローラ2
F0	コプロセッサエラー
170-177	(IDEセカンダリバス)
1F0-1F7	(IDEプライマリバス)
2F8-2FF	シリアルポート2
370-377	(フロッピーディスクコントローラ2)、IDEコントローラ2
3BF-3DF	VGA
3F0-3F7	フロッピーディスクコントローラ1、IDEコントローラ1
3F8-3FF	シリアルポート1
4D0-4D1	割り込みコントローラ1、2
CA2-CA7	ベースボードマネージメントコントローラ(BMC)
CF8-CFB	PCIコンフィグレーションアドレス/リセットコントロール
CFC-CFF	PCIコンフィグレーションデータ

*1 16進数で表記しています。
*2 PCIデバイスのI/OポートアドレスはPCIデバイスの種類や数によって任意に設定されます。

RAIDのコンフィグレーション

ここでは本装置内蔵のハードディスクドライブをディスクアレイドライブとして運用するための方法について説明します。

サポートするRAIDについて

本装置内蔵のマザーボードにあるRAIDコントローラを使用してディスクアレイ(RAID1)を構築することができます。
構築に必要となる機器はシリアルATA(SATA)ハードディスクドライブ(2台)のみです。

● RAID0(ストライピング) [本装置ではサポートしていません]

2台のハードディスクドライブに対してデータを分散して記録する方法です。この方法を「ストライピング」と呼びます。2つのハードディスクドライブへ処理を分散させることによりハードディスクドライブ単体で使用しているときに比べディスクアクセス性能を向上させることができます。

重要

- **データを2台のハードディスクドライブに分散して記録しているためアレイを構成しているハードディスクドライブが1台でも故障するとデータの復旧はできません。**
- **アレイの論理容量は、接続されたハードディスクドライブの整数倍となります。**

● RAID1(ミラーリング)

2台のハードディスクドライブに対して同じデータを記録する方法です。この方法を「ミラーリング」と呼びます。データを記録するときに同時に2台のハードディスクドライブに記録するため、使用中に片方のハードディスクドライブが故障してももう片方の正常なハードディスクドライブを使用してシステムダウンすることなく継続して運用することができます。

- **データを2台のハードディスクドライブへ同時にリード/ライトしているため、単体ディスクに比べてディスクアクセス性能は劣ります。**
- **アレイの論理容量は、接続されたハードディスクドライブ1台と同じとなります。**

ハードディスクドライブの取り付け

本体に2台のSATAハードディスクドライブを取り付けてください。取り付け手順については、340ページを参照してください。

取り付ける2台のハードディスクドライブは同じ回転速度のものを使用してください。また、RAID1を構築する場合は、同じ容量のハードディスクドライブを使用することをお勧めします。

BIOSユーティリティを使用したRAIDの有効化

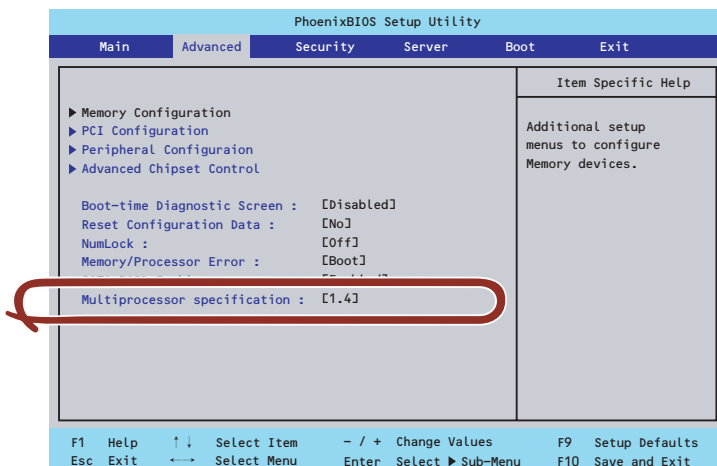
取り付けた2台のハードディスクドライブは、単一のハードディスクドライブか、2台1組で構築されるRAIDドライブのいずれかで使用することができます。
RAIDドライブとして構築するためには、BIOSセットアップユーティリティを使用して、マザーボードのSATAコネクタに接続されているハードディスクドライブをRAIDドライブとして使用するための設定が必要となります。

出荷時の設定では、単一ハードディスクドライブとして使用するように設定されています。

次の手順でBIOSセットアップユーティリティの設定を変更します。

1. BIOSセットアップユーティリティを起動する。

   詳しくは、336ページを参照してください。

2. 「Advanced」メニューから「SATA RAID Enable」の設定を「Enable」に変更する。

3. 「Exit」メニューから「Exit Saving Changes」を選択して、設定内容を保存し、BIOSセットアップユーティリティを終了する。

以上で完了です。設定を変更後、本装置を起動するたびにPOSTの画面にRAIDドライブの設定および変更をするためのユーティリティ「Array Configuration Utility(ACU)」の起動を促すメッセージが表示されます。

```
Press <Ctrl><A> for Adaptec RAID Configuration Utility
```

必要に応じてユーティリティを起動して、設定してください。詳しくはこの後の説明を参照してください。

Array Configuration Utility(ACU)を使ったRAIDの構築

ここでは、本装置を起動した後、POSTの画面から起動する「Array Configuration Utility（ACU）」を使用したRAIDの構築手順について説明します。

ACUの起動方法

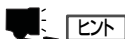
次の手順に従ってACUを起動します。

起動の前に「BIOSユーティリティを使用したRAIDの有効化」で説明しているBIOSの設定変更を完了していることを確認してください。

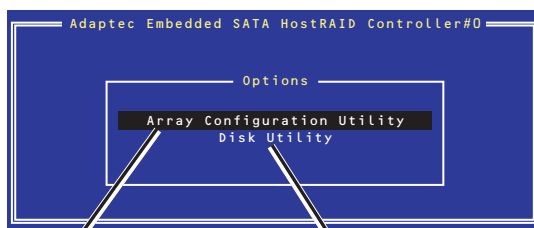
1. DianaScopeをインストールした管理PCのセットアップをする。

   本装置と通信できるセットアップが必要です。詳しくはEXPRESSBUILDER CD-ROM内のオンラインドキュメントを参照してください。

2. 本装置を起動する。
3. 管理PCのディスプレイ装置の画面に次のメッセージが表示されたら、<Ctrl>キーと<A>キーを押す。

```
Press <Ctrl><A> for Adaptec RAID Configuration Utility
```

ヒント

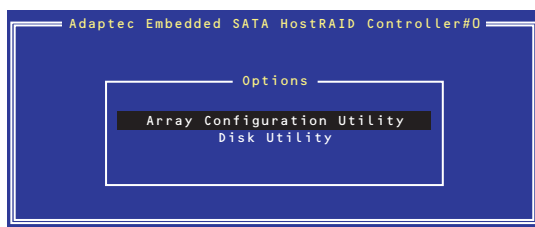
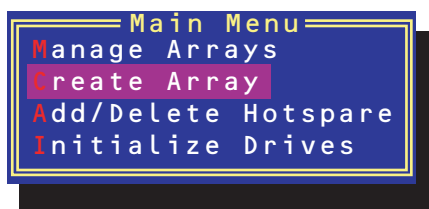
ディスプレイ装置の画面にメッセージが表示されるまでに時間がかかる場合は、本装置の電源ON後、3～5秒くらい経ってから<Ctrl>キーと<A>キーを押してみてください。

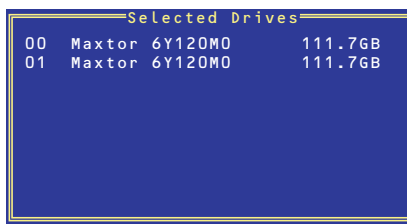
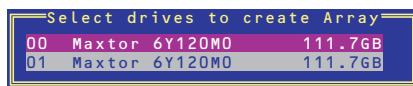
しばらくするとメインメニューが表示されます。

RAIDの構築

次の手順に従ってRAIDを構築します。

重要

- **いったんRAIDを構築してしまったドライブの属性(手順6以降に示す設定内容)を変更は変更できません。フォーマットしてやり直してください。**
- **RAIDを構築する前にRAIDドライブを構成するハードディスクドライブの物理フォーマットをしてください。物理フォーマットについては「Disk Utilitiesの使用」(395ページ)を参照してください。**

1. ACUを起動する。
2. キーボードのカーソルキーでOptionsメニューから「Array Configuration Utility」を選び、<Enter>キーを押す。

3. メインメニューから「Create Array」を選択し、<Enter>キーを押す。

4. RAIDを構築する2台のハードディスクドライブをリストから選び、<Insert>キーを押す。

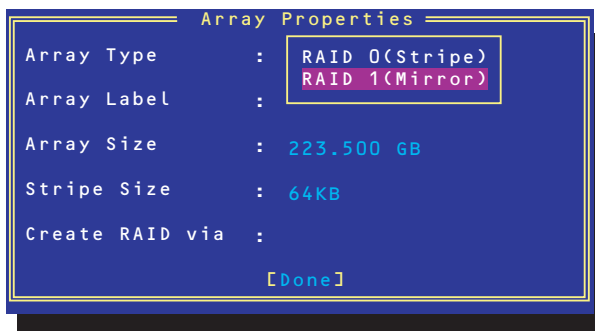
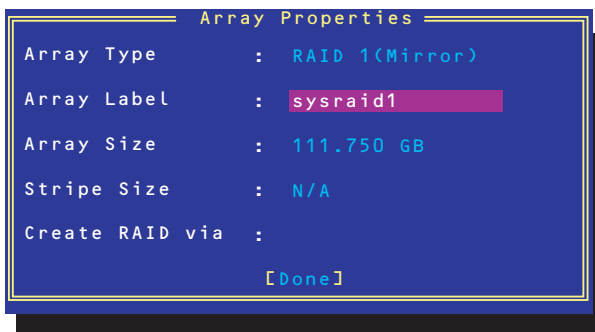
<Insert>キーを押すと、右側の「Selected Drives」リストに追加されます。削除したい場合は、左側のリストからハードディスクドライブを選択し、<Delete>キーを押すと削除され、右側のリストから消えます。

ヒント

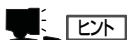
- 本装置は、最大2台のハードディスクドライブをマザーボードのSATAコネクタに接続することができます。RAIDを構築するために必要なハードディスクドライブは2台以上です。したがって、リストに表示されている2台のハードディスクドライブを選択してください。
- リストに表示されているハードディスクドライブ名がグレイに表示されているものは、使用できるディスク領域がないものか、イニシャライズされていないハードディスクドライブであることを示します。<Esc>キーを数回押してこのメニューをいったん終了して、この後の説明にある「ハードディスクドライブのイニシャライズ(394ページ)」を参照してください。

5. <Enter>キーを押す。

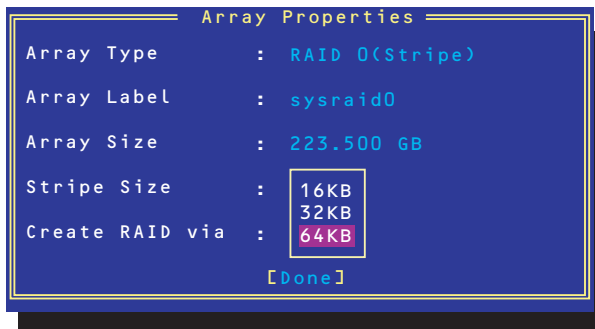
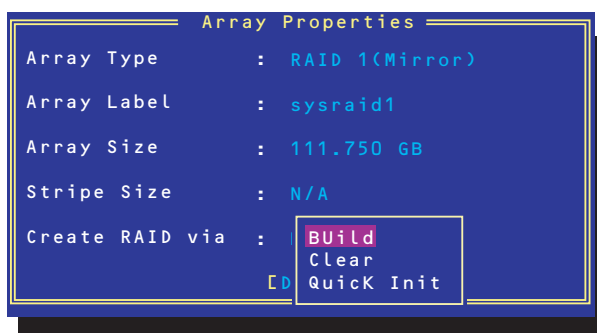
   RAIDの詳細設定を行う「Array Properties」画面が表示されます。

6. カーソルキーでRAIDレベルを選択し、<Enter>キーを押す。

   選択できるRAIDレベルはRAID0(ストライピング)とRAID1(ミラーリング)のいずれかですが、本装置ではRAID1のみをサポートしています。

7. 作成するRAIDドライブのボリュームラベル名を入力し、<Enter>キーを押す。

8. <RAID0を選択した場合のみ>

   ストライプサイズを16KB、または32KB、64KB(初期設定)から選択し、<Enter>キーを押す。

   ヒント

   - この手順はRAID0を選択した場合のみのものです。本装置はRAID1のみをサポートしているためこの手順は必要ありません。
   - ストライプサイズは、初期設定の64KBを選択することをお勧めします。

Array Properties
Array Type : RAID 0(Stripe)
Array Label : sysraid0
Array Size : 223.500 GB
Stripe Size :
16KB
32KB
64KB
Create RAID via :
[Done]

9. 「Create RAID via」でRAIDドライブの作成方法を選択し、<Enter>キーを押す。

「Create RAID via」では、RAIDレベル(Array Type)との組み合わせでさまざまなRAIDドライブの作成方法を指定することができます。詳細を下表に示します。

RAIDレベル	Create RAID viaの選択肢	作成方法
RAID0（本装置ではサポートしていません）	No Init	新規でRAID0ドライブを作成します。
RAID0（本装置ではサポートしていません）	Migrate	データが保存されている既存のドライブに対して新規ドライブを追加するマイグレーション（移行）をします。本装置では「Migrate」をサポートしていません。
RAID1	Build	データが保存されている既存のドライブの内容を新規ドライブにコピーし、RAID1ドライブを作成します。
RAID1	Clear	すべての内容をクリアして、新規でRAID1ドライブを作成します。
RAID1	Quick Init	新規でRAID1ドライブを即座に作成します。

RAID0は本装置ではサポートしていません。

- 既存のRAIDドライブに新規ドライブを追加する場合は、あらかじめ新規ドライブ内のデータのバックアップをとっておいてください。
- ACUを使ってRAID1ドライブの作成中、その処理を中断すると、ACUを使って処理を再開させることはできません。
- Quick InitでRAID1ドライブを作成すると、その後の整合性チェック(Consistency Check)で不整合を通知される場合がありますが、ハードディスクドライブの故障やRAIDドライブの構築を失敗したわけではありません。
- RAID1を構成するハードディスクドライブのディスク容量が異なっていてもRAID1ドライブを構築することができます。ただし、「Build」オプションでRAID1ドライブを作成する場合、容量の小さい方のハードディスクドライブをコピー元または第1ドライブに指定してください。

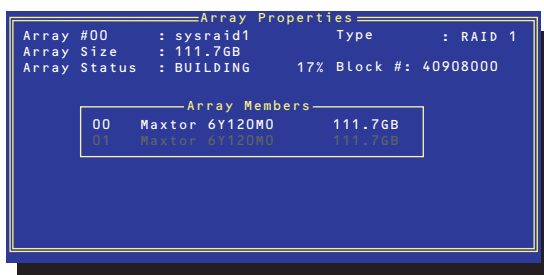
10. 「Source Drive」を選択して、<Enter>キーを押す。

```
Select Source Drive
00   Maxtor 6Y120M0     111.7GB
01   Maxtor 6Y120M0     111.7GB
```

11. すべての設定を完了したら、「Done」を選択して、<Enter>キーを押す。

RAIDの作成処理が始まります。完了までしばらくお待ちください。

```
Array Properties
Array #00      : sysraid1          Type          : RAID 1
Array Size     : 111.7GB
Array Status   : BUILDING       17% Block #: 40908000

              Array Members
  00    Maxtor 6Y120M0         111.7GB
  01    Maxtor 6Y120M0         111.7GB
```

ディスクアレイの管理

オプションメニューから「Array Configuration Utility」を選択して表示されるメインメニューで、「Manage Arrays」を選択すると、RAIDドライブの設定(属性)情報の確認やRAIDドライブ(アレイ)の削除をすることができます。

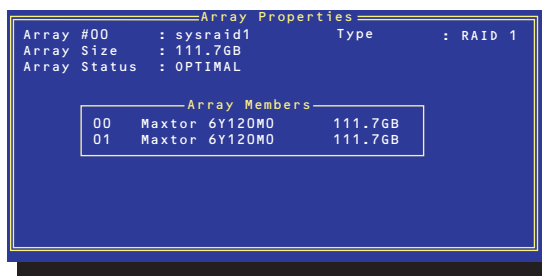
```
Main Menu
Manage Arrays
Create Array
Add/Delete Hotspare
Initialize Drives
```

● **アレイ情報の確認**

Main Menuで「Manage Arrays」を選択し、<Enter>キーを押すとアレイを構築しているRAIDドライブの一覧が表示されます。

RAIDドライブを選択し、<Enter>キーを押してください。選択したRAIDドライブに関するプロパティダイアログボックスが表示されます。このプロパティダイアログボックスにはRAIDドライブを構成している物理ハードディスクドライブの情報も含まれます。

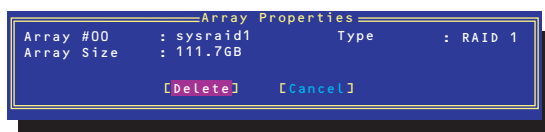
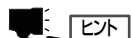
```
Array Properties
Array #00      : sysraid1          Type          : RAID 1
Array Size     : 111.7GB
Array Status   : OPTIMAL

              Array Members
  00    Maxtor 6Y120M0         111.7GB
  01    Maxtor 6Y120M0         111.7GB
```

<Esc>キーを押すと1つ前の画面に戻ります。

● アレイの削除

本装置でアレイの削除を実行すると、システム全体のデータを消去してしまいます(システムの再インストールがやさまざまなデータのリストア作業などが必要となります)。アレイを削除する前にRAIDドライブ内の大切なデータをバックアップしてください。削除を実行するとすべてのデータを消失します。また、消失したデータを復帰(リストア)させることはできません。

メインメニューで「Manage Arrays」を選択し、<Enter>キーを押すとアレイを構築しているRAIDドライブの一覧が表示されます。以降の削除手順を以下に示します。

1. 削除するRAIDドライブを選択し、<Delete>キーを押す。
2. プロパティダイアログボックスで、「Delete」を選択し、<Enter>キーを押す。

削除についての警告メッセージが表示されます。

表示メッセージの内容や数はRAIDレベルによって異なります。

3. 「Yes」を選択する。

   アレイやパーティションが削除されます。「No」を選択すると1つ前の画面に戻ります。

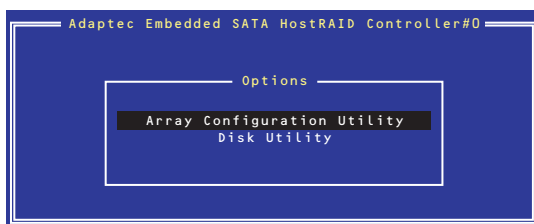
4. <Esc>キーを押して1つ前の画面に戻る。

ハードディスクドライブのイニシャライズ

RAIDドライブを作成するためにはハードディスクドライブがイニシャライズされていなければなりません(イニシャライズされていないハードディスクドライブは、RAIDドライブを構築するドライブの選択画面でリストに表示されないか、グレーアウトされて表示されます)。

- **イニシャライズを実行するとハードディスクドライブ上のパーティションテーブルを上書きし、データを書き込めない状態にします。**
- **アレイとして使用していたハードディスクドライブをイニシャライズすると、再び元のアレイに戻すことはできません。**
- **起動ドライブとして使用しているRAID0ドライブを構成するハードディスクドライブをイニシャライズするとシステムが起動できなくなります。**

次の手順でハードディスクドライブをイニシャライズします。

1. ACUを起動する。
2. キーボードのカーソルキーでOptionsメニューから「Array Configuration Utility」を選び、<Enter>キーを押す。

3. メインメニューから「Initialize Drives」を選択し、<Enter>キーを押す。

Main Menu
Manage Arrays
Create Array
Add/Delete Hotspare
Initialize Drives

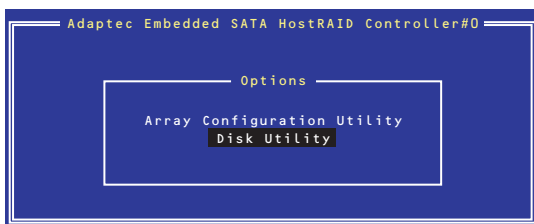
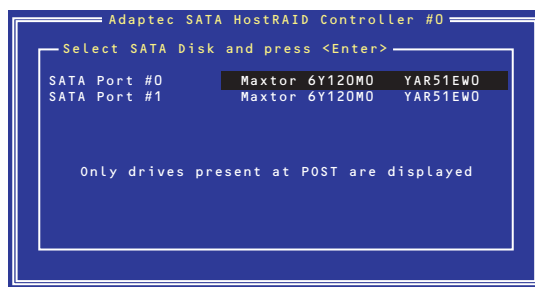
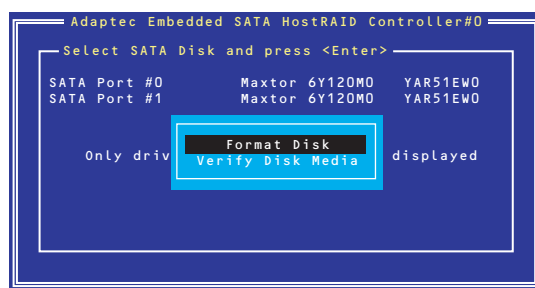
4. カーソルキーを使ってリストからイニシャライズをするハードディスクドライブを選び、<Insert>キーを押す。
5. もう一方のハードディスクドライブを手順4と同様の手順で選択する。
6. <Enter>キーを押す。
7. 警告メッセージの内容を読み、イニシャライズするハードディスクドライブを正しく選択していることを確認し、<Y>キーを押してイニシャライズを続ける。

Disk Utilitiesの使用

ACUを起動後に表示されるオプションメニューにある「Disk Utilities」は、ハードディスクドライブのローレベルフォーマットやベリファイをする場合に使用するメニューです。

1. ACUを起動する。

   詳しくは、「ACUの起動方法(389ページ)」を参照してください。

2. キーボードのカーソルキーでOptionsメニューから「Disk Utilities」を選び、<Enter>キーを押す。

3. 目的のハードディスクドライブを選択し、<Enter>キーを押す。

4. 実行したいメニューを選択し、<Enter>キーを押す。

– Format Disk
直ちに対象としているハードディスクドライブをローレベルでフォーマットします(ゼロ埋め込み)。購入時のSATAハードディスクドライブは工場出荷時にローレベルでフォーマット済みですが、RAIDを構成するハードディスクドライブは、RAIDを構築する前にこのオプションを使ってフォーマットをしてください。

重要

ローレベルフォーマットはハードディスクドライブ内のすべてのデータを消去します。フォーマットを実行する前にハードディスクドライブ内にある大切なデータのバックアップをとってください。

– Verify Disk Media
ハードディスクドライブ内のメディア不良を検出します。

RAIDの保守と管理(Adaptec Storage Manager - Browser Edition)

Adaptec Storage Manager™ Browser Edition(以降、「ASMBE」と呼ぶ)は、本体標準装備のHostRAID(SATA)を利用したRAIDドライブの保守・管理をするためのWebベースのアプリケーションであり、ブラウザでのグラフィカルな画面による操作ができます。

重要 **Linux上でASMBEを使用する場合には、ASMBEに同梱されているブラウザ(Mozilla 1.2b)を使用してください。**

ASMBEをインストールすると、以下の機能が使用できるようになります。

- 冗長性アレイが縮退(Degraded)状態になった場合のリビルド(復旧)機能
- アレイの整合性をチェックするためのVerify機能

ASMBEは本装置にインストールします。ネットワーク上の管理コンピュータからASMBEにアクセスするには前記のブラウザが必要です。また、コンピュータの間はTCP/IPを経由した通信ができるよう設定していなければなりません。このTCP/IPを経由する通信では、SHTTPまたはSSLをセキュリティとデータ転送の暗号化のために使用しています。

ASMBEのインストール

次の手順に従ってASMBEをインストールします。インストールに必要なファイルは、本装置に添付の「バックアップCD-ROM」の以下に収録されています。

/nec/Linux/ASMBE/HostRAID/HR_InstallASMBE-1.00.tar.gz

重要 **ASMBEのインストールはroot権限を持ったユーザーで行ってください。**

1. ASMBEのインストールファイル「HR_InstallASMBE-1.00.tar.gz」を任意のディレクトリにコピーする。

   #cp HR_InstallASMBE-1.00.tar.gz　コピー先

   例）　cp HR_InstallASMBE-1.00.tar.gz /tmp/.

2. コピーしたファイルを展開する。

   #cd コピー先

   例）　#tar -zxvf HR_InstallASMBE-1.00.tar.gz

3. ファイル展開後、インストールコマンドを実行する。

   #./instasmbe

4. インストールの最後に以下の表示が出ていることを確認する。

   Installation Complete

   重要

   インストールコマンドを実行した際に以下のエラーメッセージが表示され、インストールが失敗する場合があります。この場合は、エラーメッセージ内に必要なパッケージが表示されますので、表示されたパッケージをインストールしてから、再度ASMBEのインストールコマンドを実行してください。

   表示メッセージ(必要なパッケージが「ZZZZZZZZZZ」に表示されます)

   ```
   Error: Failed dependencies:
           XXXXXXXXXX is needed by YYYYYYYYYY
           Suggested resolutions:
           ZZZZZZZZZZ
   ```

   ASMBEのインストールに必要なパッケージは2つ以上ある場合があります。必要なパッケージはすべてインストールしてください。また、これらの必要なパッケージをインストールする際にも他のパッケージのインストールを要求される場合がありますので同様にインストールしてください。

5. システムを再起動する。

6. ASMBE-RENICEファイル「asmbe-renice-1.00-00.tar.gz」を任意のディレクトリにコピーする。

   #cp asmbe-renice-1.00-00.tar.gz コピー先

   例) cp asmbe-renice-1.00-00.tar.gz /tmp/.

7. コピーしたファイルを展開する。

   #cd コピー先
   #tar -zxvf asmbe-renice-1.00-00.tar.gz

8. ファイル展開後、インストールを実行する。

   #rpm -ivh asmbe-renice-1.00-00.i386.rpm

9. システムを再起動する。

以上でASMBEのインストールは完了です。

システム起動後にASMBEのデーモン(arcpd)が起動されると、CPU使用率が100%近くになりますが、上記のASMBE-RENICE(asmbe-renice-1.00-00.i386.rpm)をインストールすることにより、他プロセスへの影響を軽減することができます。

操　作

ASMBEの起動方法や表示される画面操作方法などについて説明します。

ASMBEの起動

ASMBEの起動(ASMBEへのログオン)には、本装置にコンソールを直接接続して行う「ローカル」と管理コンピュータからネットワークを介して接続する「リモート」の2つの方法があります。

- **複数のWebブラウザから同時に制御しないでください。**
- **ASMBEは操作する時以外は、閉じておいてください。**

使用しているOS、およびブラウザ、カラースキームにより、説明中の画像が実際の画面と異なる場合があります。

どちらの方法においても、初めての起動ではセキュリティのために「証明書」を作成します。「始めてログオンする場合」をあらかじめ参照してセキュリティの設定をしてください。

始めてログオンする場合

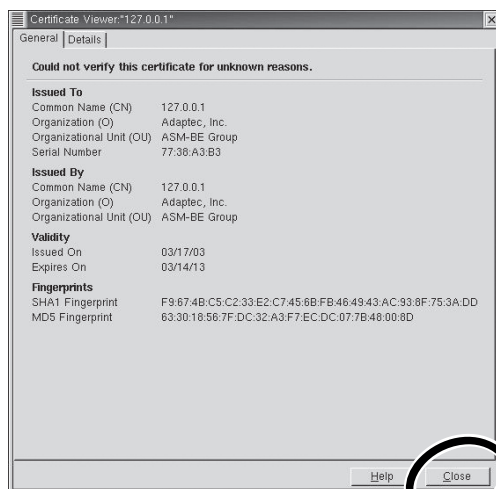
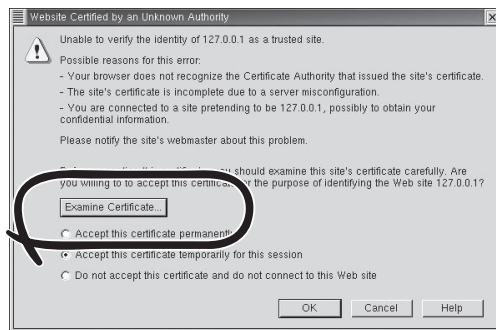
初めてASMBEを起動すると、セキュリティの警告が表示されます。

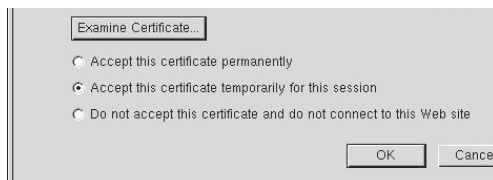
以下の手順を行ってセキュリティに関する設定を行ってください。

1. 「Examine Certificate...」をクリックする。

   「Certificate Viewer」が開き証明書が表示されます。

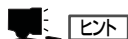
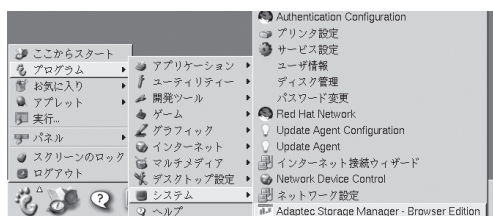
2. 内容を確認した後、[Close]をクリックする。

   セキュリティの警告画面に戻ります。

3. 証明書を受け入れる場合には[Accept this certificate permanently]をチェックして[OK]をクリックする。

   一時的に受け入れる場合には[Accept this certificate temporarily for this session]をチェックして[OK]をクリックします。一時的に受け入れる場合には、次回ログオン時にもセキュリティの警告が表示されます。

以上でセキュリティに関する設定は終了です。

ローカルから起動する

1. 「メインメニュー」→「プログラム」→「システム」を選択し、「Adaptec Storage Manager - Browser Edition」をクリックする。

   ログオン画面が表示されます。

上記のメニューに「Adaptec Storage Manager - Browser Edition」が存在しない場合はMozilla Webブラウザより以下のURLを指定してください。

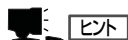
https://(IPアドレス):3513/Adaptec

例) Red Hat Enterprise Linux 3 AS EM64Tの場合、Mozilla Webブラウザは以下のパスから起動できます。

「メインメニュー」→「インターネット」→「Mozilla Webブラウザ」

2. 各フィールドに入力して、[Login]をクリックする。

   [Hostname]フィールドには、管理するシステムのホスト名またはIPアドレスを入力します。

   [Username]フィールドと「Password」フィールドには管理するシステムのroot、もしくはwheelグループに所属するユーザー名とそのパスワードを入力します。

wheelグループにユーザを登録することでroot以外のユーザーでASMBEを操作することができます。

リモートから起動する

ASMBEをMozilla上で使用する場合の準備

Mozillaの設定でJavaScriptおよびCookiesが無効になっている場合、ASMBEが正常に動作しないことがあります。以下の設定でJavaScriptおよびCookiesを有効にしてからASMBEを使用してください。

1. Mozillaの「Edit」の「Preferences...」をクリックし、「Privacy & Security」→「Cookies」ダイアログボックスを表示する。
2. 「Disable cookies」がチェックされている場合、「Enable cookies for the originating web site only」もしくは「Enable all cookies」にチェックしてCookiesを有効にする。
3. 「Advanced」→「Scripts & Plugins」ダイアログボックスを表示する。
4. 「Navigator」にチェックを入れ、[OK]をクリックし、JavaScriptを有効にする。
5. 「Allow scripts to:」の以下の項目にチェックを入れ、[OK]をクリックし、スクリプトを許可する。
   - Open unrequested windows
   - Move or resize existing windows
   - Raise or lower windows
   - Hide the status bar
   - Change status bar text
   - Change images
   - Create or change cookies
   - Read cookies

プロキシサーバを使用している場合は下記のようにプロキシサーバはバイパスしてください。

1. Mozillaの「Edit」の「Preferences...」をクリックし、「Advanced」→「Proxies」ダイアログボックスを表示する。
2. 「Direct connection to the Internet」がチェックされている場合は[OK]をクリックして終了する。
3. 「Manual proxy configuration」がチェックされている場合は「No Proxy for:」の欄に制御するZCR/HostRAIDのIPアドレスを入力し、[OK]をクリックする。

1. Webブラウザを起動する。

2. ブラウザのアドレスに制御するZCR/HostRAIDのIPアドレスを入力し、<Enter>キーを押す。

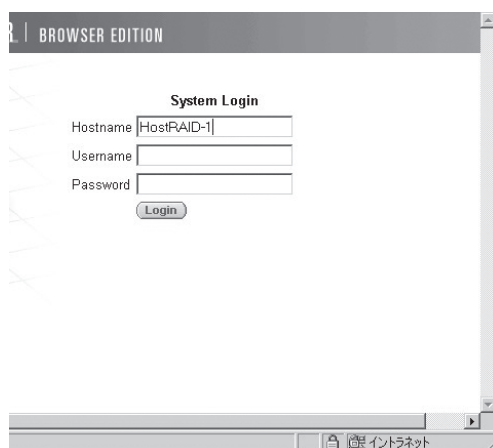
IPアドレスが「10.10.10.10」の場合は、「https://10.10.10.10:3513/Adaptec」と入力してください。
リモートシステムとのセッションが開設できたとき、ASMBEのログオン画面が表示されます。

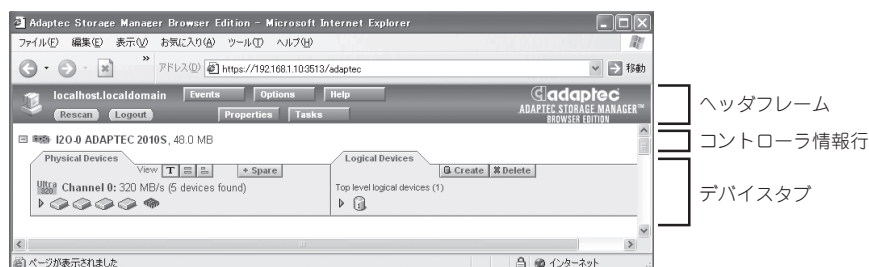
ヒント

インターネットへのアクセスにプロキシサーバを使用している場合はプロキシサーバをバイパスしてください。設定方法は前述の「ヒント」を参照してください。

3. 各フィールドに入力して、[Login]をクリックする。

[Hostname]フィールドには、管理するシステムのホスト名またはIPアドレスを入力します。

[Username]フィールドと「Password」フィールドには管理するシステムのroot、もしくはwheelグループに所属するユーザー名とそのパスワードを入力します。

操作画面

ASMBEの表示例を以下に示します(起動時には以下のような画面を表示します)。

ASMBEウィンドウにはヘッダフレーム、コントローラ情報行、デバイスタブがあります。

- **ヘッダフレーム**

  以下のボタンや操作中のシステム名を表示します。

  - [Logout]をクリックするとセッションは終了し、ログオン画面に戻ります。
  - [Rescan]はシステムのコンフィグレーションを再度読み込むために使用します。アレイの作成後などは自動的に再スキャンを実施しますが、システムとASMBEの表示に不整合があった場合はこの[Rescan]を行ってください。
  - [Events]、[Option]、[Help]、[Properties]、[Tasks] をクリックすると、新たにウィンドウを開いて、各種設定変更、操作、詳細情報の表示を行うことができます。「イベント」、「ユーザインタフェースオプション」、「ヘルプ」、「プロパティの表示と変更」、「タスクの作成と表示」でそれぞれの説明を行っています。

- **コントローラ情報行**

  ヘッダフレームの直後にコントローラのモデル番号を表示します。左端に[⊟]ボタンがある場合、このボタンをクリックするとこのコントローラの情報の表示を最小化することができます。

● **デバイスタブ**

コントローラ情報に続いて、「Physical Devices」タブと「Logical Devices」タブを表示します。「Physical Devices」タブには、コントローラに接続されたデバイスの情報を表示します。「Logical Devices」タブには、作成済みのアレイの情報を表示します。

コントローラ情報行をクリックしてコントローラを選択すると、[Properties]、[Tasks]がブルーからアンバーに変わります。このボタンをクリックすると新たにウィンドウが開いてコントローラのオプション仕様や詳細情報を表示することができます。
マウスカーソルをデバイスアイコンやボタン上に合わせると、ヒントをポップアップ表示します。ボタンのヒントはそのボタンの機能を表示します。一方、デバイスのヒントは付加的な情報を表示します。

重要

- **システムの状態とASMBEの表示に不整合が起こる場合があります。その場合は[Rescan]をクリックしてASMBEの表示を最新の状態にしてください。**
- **システム起動時に、ASMBEのGUI画面でアレイのアイコンやハードディスクのアイコンがOptimalであることを確認してください。アイコンがOptimal以外の場合はハードディスクドライブの交換が必要な可能性があります。ただし、アラート通報が行われない場合があるため、保守員に連絡してハードディスクドライブの交換を行ってください。**
- **Degraded状態のアレイの修復を行った後はASMBEのGUI画面でアレイのアイコンがoptimalの状態になっていることを確認してください。通報されない場合があります。**

物理デバイス

「Physical Devices」タブにはZCR/HostRAIDに接続されたハードディスクドライブなどのデバイスに関連する情報を表示します。デバイスはチャネルごと、番号順に表示します。
検出したデバイス、コントローラのチャネル数、最大転送能力をチャネルごとに表示します。
チャネルまたはデバイスアイコンを選択すると、[Properties]や[Tasks]がアンバーに変化します。この状態で、これらのボタンをクリックすると、新たにウィンドウが開いてデバイスやチャネルのオプション仕様や詳細情報を表示することができます。

ホットスペア

[+ Spare]をクリックして、ホットスペアを設定することができます。ホットスペアは冗長アレイのハードディスクドライブが故障したときにこのアレイを保護するために使います。すなわち、冗長アレイのハードディスクドライブが故障した場合、アレイを保護するために、ホットスペアにリビルドを行って、故障ハードディスクドライブの代替をします。

表　示

「Physical Devices」タブには次の3つのビュー選択ボタンがあります。選択したビュー選択ボタンの色は他の2つのボタンよりも明るい青色になります。

[T]　テキスト記述による表示(デフォルトの表示です)

[ ]　フルサイズの容量表示

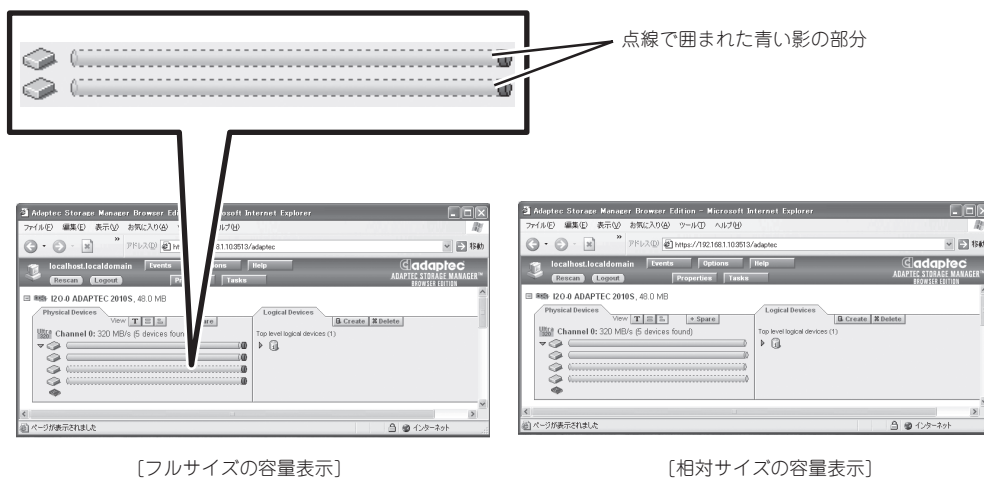
[ ]　相対サイズの容量表示

表示が要約されている場合、どのビューの表示も同様です。ボタンをクリックして表示モードを変更した場合、黄色の矢印がデバイス行の左端で点滅して、詳細表示への変更を促します。

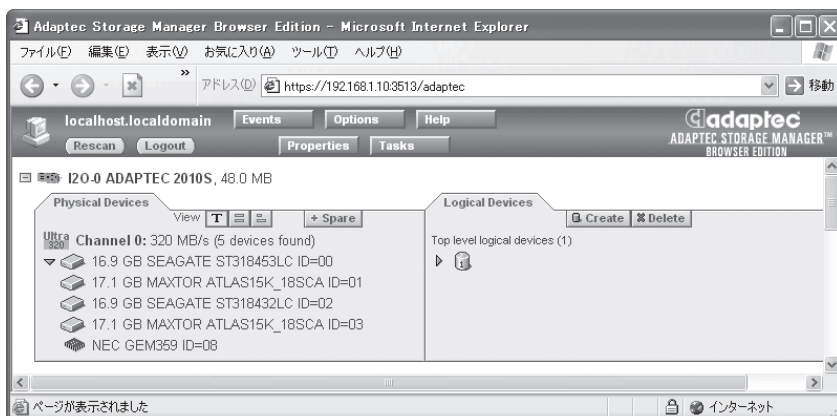
「テキスト記述による表示」で詳細表示を行うと、デバイスごとに以下の情報を表示します。

- デバイスの容量
- デバイスの製造元やモデル番号
- SCSI ID

「フルサイズの容量表示」や「相対サイズの容量表示」で詳細表示を行うと、それぞれのデバイスの情報をバーで表示することができます。点線で囲まれた青い影の部分はアレイとして使っていない部分です。

〔フルサイズの容量表示〕　〔相対サイズの容量表示〕

「フルサイズの容量表示」は容量に関わらずデバイスごとに同じ長さのバーを表示し、「相対サイズの容量表示」は、容量をデバイスの容量に比例した長さのバーを表示します。どちらの場合も、アレイに使用している部分は、バーをグレイのセグメントで示しています。グレイのセグメントを選択すると、「Logical Devices」タブにおいて、このセグメントがメンバになっているアレイが強調表示になります。また、バーに小さな暗いグレイ表示の部分があれば、そこは、予約された領域です。

デバイス表示の変更

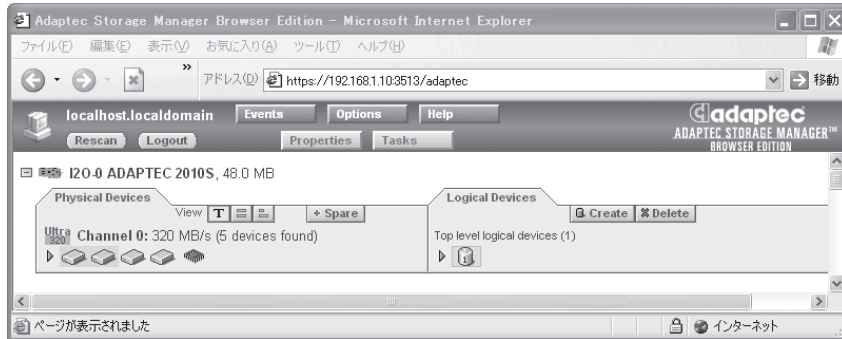
ASMBEを起動した直後の「Physical Devices」タブの情報は「テキスト記述による表示」でデバイスの情報を要約した表示です。この表示で、マウスをデバイスアイコン上に重ねるか、またはデバイスアイコン表示列の左端の[▷]をクリックすると、要約されて表示されていない情報を表示することができます([▷]をクリックすると、下図のような詳細表示になります)。

[ ]アイコンはハードディスクドライブアイコンです。+シンボルがハードディスクドライブアイコンに表示されていれば、このハードディスクドライブはホットスペアのハードディスクドライブです。これ以外のアイコンは他のデバイスを示しています。

論理デバイス

「Logical Devices」タブには[Create]と[Delete]があります。
[Create]や[Delete]をクリックすると、アレイの作成やアレイの削除のためのそれぞれのウィザードを起動することができます。詳細は「アレイの作成」や「アレイの削除」で説明します。
「Logical Devices」タブにはこのコントローラに作成したアレイのアイコンを表示しています。

アレイアイコンの表示方法には要約表示と詳細表示の2種類があります。要約表示の場合は、それぞれのアレイのRAIDレベルとホットスペアによる保護の有無を表示することができます。
詳細表示の場合は、アレイのアイコンとその容量、名前、RAIDレベルを縦に並べて表示します。

要約表示、詳細表示のどちらの場合もアレイのアイコンをクリックして選択すると、以下の項目がアンバーで強調表示になります。

- 「Physical Devices」タブに表示しているアレイを構成するハードディスクドライブやセグメント
- ヘッダフレームの[Properties]と[Tasks](このボタンをクリックすると、新たにウィンドウを開いて、そのアレイのオプション仕様や詳細情報を表示することができます)

アレイの作成

本装置に対してASMBEを使ったアレイの作成はできません。

リビルドの実施

リビルドは、電源をOFFにして新しいハードディスクドライブに交換した後、システムおよびASMBEを起動してホットスペアを作成することで、自動復旧させることです。

ハードディスクドライブを交換する場合は、システムの電源をOFFにした状態で交換してください(360ページ参照)。また、交換するハードディスクドライブはASMBE画面にて接続されているPort番号を確認してから実施することをお勧めします。

容量の小さいアレイに対してリビルドを実施してもRebuildの表示が現れない場合があります。この場合、リビルドの終了確認は[Events]をクリックして表示されるイベントログにて確認してください。

以下の手順でホットスペアを作成し、リビルドを実施します。

1. [Physical Devices]タブの[+ Spare]をクリックする。
2. [Physical Devices]タブにあるホットスペアに設定するデバイスアイコンを選択する。
3. [Finish]をクリックする。

ホットスペアの作成と削除

ホットスペアの作成と削除の手順について説明します。

ホットスペアの作成

本装置でホットスペアを作成するのは、リビルドをする場合のみです。それ以外の目的でホットスペアドライブを作成することはできません。リビルドのためにホットスペアを実行する場合は、前ページの「リビルドの実施」を参照してください。

ホットスペアを作成する場合、以下のハードディスクドライブは使用しないでください。アレイが縮退状態の時にホットスペアを作成してもリビルドを開始しない場合があります。

- **すでにアレイで使用しているハードディスクドライブ**
- **パーティションが作成済みのハードディスクドライブ**

ホットスペアの削除

以下の手順でホットスペアを削除します。

1. [Physical Devices]タブの[+ Spare]をクリックする。
2. [Physical Devices]タブにあるホットスペアを削除するデバイスアイコンを選択する。
3. [Finish]をクリックする。

   削除が完了すると、デバイスアイコンに表示していた「+」が消えます。

アレイの削除

以下の手順でアレイを削除することができます。

重要

OSのパーティションが作成されているアレイを削除することはできません。また、本装置ではひとつのアレイのみが存在する設定のため削除はできません。

1. [Logical Devices]タブの[Delete]をクリックする。

2. [Logical Devices]タブの削除するアレイを選択する。

3. [Finish]をクリックする。

4. 確認ダイアログボックスで[OK]をクリックする。

イベント

[Events]をクリックするとサポートしているコントローラすべてのイベントメッセージを表示することができます。
[Event View]タブでは以下の情報をイベントごとに表示します。

- イベントが発生した時間
- イベントの重要度
- イベントメッセージ

デフォルト(All)の場合はすべてのイベント(CriticalおよびWarning、Informational)を表示しますが、ドロップダウンリストで「Critical」または「Warning」を選択すると、それぞれのレベルのイベントだけ表示することができます。
イベントログをクリアするためにはウィンドウの下側にある[Clear Log]をクリックします。
イベントログを保存するためには[Save Log]をクリックします。保存されたログファイルはWebブラウザで閲覧できます。
[Event Notification]タブでは、イベント通知に関するさまざまな設定を行います。

- **System Log**

  システムログに追加するレベルを設定します。デフォルトはAll eventsです。

- **Popup Alerts**

  ポップアップで警告するレベルを設定します。デフォルトはNoneです。

- **Sound On**

  ポップアップ警告の際、警告音を鳴らす場合はチェックボックスをチェックします。デフォルトはチェックされていません。

- **E-mail Alerts**

  E-mail通報はサポートしていません。システムイベントログのメッセージ通報については、ESMPRO/ServerAgentのアラートマネージャを使用してください。

[Event Notification]タブのSystem LogとPopup Alertsの設定は変更しないでください。

ASMBEのイベントログに、毎日AM2:00台に下記のメッセージが登録されることがあります。

Informational [IOM0032] Test all spares started

Informational [IOM0005] No spares available to test

運用に影響はありませんので、これらのメッセージは無視してください。

ユーザーインタフェースオプション

[Options]をクリックすると、ASMBEのユーザインタフェースを変更することができます。変更はドロップダウンリストから選択することで有効になります。
以下の項目を変更できます

- **Background Update Frequency**

  ASMBEの表示の更新間隔を変更します。デフォルトは30秒で、他に15秒、1分、5分が選択可能です。

- **Highlight on Mouseover**

  ASMBE画面のアレイまたはデバイス、チャネル、コントローラのアイコンにマウスカーソルを位置させると、このアイコンをアンバー色の枠で囲って表示することができます。

  Yes: 有効(デフォルト)
  No: 無効

- **Popup Tool Tips**

  マウスカーソルを移動させ、デバイスまたはボタンの上にカーソルを位置づけたときに、ポップアップで情報を表示することができます。ボタンの場合は、そのボタンが持つ機能に関する情報を表示します。デバイスの場合は、追加情報を表示します。

  Delayed: 短時間の遅延の後に情報を表示します(デフォルト)
  Off: 機能を無効にする
  Immediate: ただちにポップアップを表示する

ヘルプ

[Help]をクリックすると「This Application」のタブを持つウィンドウが開きます。
「This Application」タブでは、アプリケーションのバージョンや名前についての情報を表示します。

プロパティの表示と変更

ASMBEの画面上でデバイスなどの詳細情報を[Properties]をクリックして表示することができます。コントローラやチャネル、デバイス、アレイのアイコンを選択し、[Properties]をクリックすると、それぞれの詳細情報を表示します。
[Properties]がアンバー表示のときにこのボタンをクリックすると、新たなウィンドウが開いて、選択した項目についての詳細情報やオプションを表示することができます。
[Properties]が青色表示のときにこのボタンをクリックすると、接続しているシステムのホスト名を表示することができます。
変更可能フィールドを選択したときは、[Apply]や[Cancel]が表示されプロパティを変更することができます。

コントローラプロパティ

コントローラを選択し、[Properties]をクリックすると、「Controller Info」や「Details」のタブから構成されるウィンドウを表示します。

- **Controller Infoタブ**

選択したコントローラの以下の情報を表示します(ZCR/HostRAIDによって表示される項目は違います)。

Model: コントローラのモデル番号
Serial number: コントローラを識別するユニークな番号
Host bus: コントローラが接続されているバスの番号と形式
Memory Size: メモリのサイズ
Cache Size: キャッシュのサイズ
channels: コントローラのチャネル(SCSIまたはATA)数
Ports: コントローラのポート数

- **Detailsタブ**

このコントローラのコンポーネントの以下の情報を表示します。

Kernel Version: コントローラが動作するためのソフトウェアのバージョン
Hardware Version: コントローラハードウェアのバージョン
Processor: プロセッサのタイプ

チャネルプロパティ

チャネルを選択し、[Properties]をクリックすると以下の情報を「Channel Info」タブに表示します。

Channel Type: SCSIまたはATAなどのチャネル種別

Max Data Rate: このチャネルの最大転送能力(320MB/sなど)

物理デバイスプロパティ

デバイスを選択し、[Properties]をクリックした場合は、「Drive Info」および「Capacity」、「S.M.A.R.T」タブ付きのウィンドウで以下の情報を表示します。

- **Drive Infoタブ**

Status:	デバイスの状態を表示する。状態は、Optimal(正常)、Failed(故障)、SMART、Warning(警告)で表示
Type:	Disk Drive、CD-ROM、Scanner、Printerなどのようなデバイスのクラスを表示
Product:	製造元によってデバイスに与えられた製品名
Vendor:	このデバイスの製造元
Revision:	このデバイスのバージョン番号
Data Rate:	このデバイスがサポートしている最大転送スピード
SCSI ID、LUN:	SCSIチャネルの場合SCSI IDとデバイスのLUN

- **Capacityタブ**

ハードディスクドライブの場合に「Capacity」タブを表示します。ハードディスクドライブの総容量や「Reserved」、「Used」、「Available」などの状態を表示します。容量は512バイトブロックの数(10進数と16進数の両方で表示)とキロバイト、メガバイト、ギガバイトのいずれかの容量を表示します。

「Detailed」を選択すると、ハードディスクドライブのすべてのセグメント情報を表示します。この表示は、以下の情報をそれぞれのセグメントごとに表示します。

- セグメント番号
- 開始と終了のブロック
- セグメントサイズとタイプ

タイプはセグメントの使われ方を示します。最初と最後のセグメントはいつも予約済みです。ハードディスクドライブの先頭にはコントローラのRAIDシグネチャを格納しています。ハードディスクドライブの終了は100メガバイト単位に丸められた容量です。

セグメントがアレイのコンポーネントの場合、そのアレイレベルを示します。セグメントがアレイの使用領域でも予約領域でもない場合は、「Available」と表示しています。

詳細な表示は10進数でセグメントの開始と終了ブロック番号を表示しますが、ドロップダウンリストの選択によって16進数または容量のどちらかの番号表示に変更することができます。

- **S.M.A.R.Tタブ**

SMART障害断定通報をサポートしているハードディスクドライブについては、このタブで以下を表示します。

Enable:	このデバイスでSMART報告が有効/無効を示す。
Predictive Failure Occurred:	このデバイスで障害報告が行われたか否かを示す。

論理デバイスプロパティ

論理デバイスアイコンを選択して、[Properties]をクリックすると、「Logical Device Info」タブ付きのウィンドウを表示します。

● 「Logical Device Info」タブ

「Logical Device Info」タブには以下の情報を表示します。

Status:	アレイの状態を表示する。状態はOptimal(正常)またはDegraded(縮退)、Offline(オフライン)、Failed(故障)で表示します。
Name:	アレイの名前を表示します。このフィールドは変更可能です。
Type:	選択したアレイのボリュームタイプまたはRAIDレベル。
Capacity:	アレイの容量。カッコ内にブロック数を表示します。
Stripe Size:	選択したアレイのストライプサイズ。
Hot Spare:	選択したアレイにホットスペアが割り当てられているかを示します。
Logical Drive#:	選択したアレイにコントローラによって割り当てられた番号。この番号は、コントローラによってのみ使われます。

タスクの作成と表示

[Tasks]をクリックすると「Task Viewer」と「New Task」の2つのタブを持つウィンドウを表示します。

● 「Task Viewer」タブ

システムや選択したコントローラ、チャネル、アレイ、ハードディスクドライブに対する現在動作中のタスクやスケジュールされたタスクの詳細を表示します。

● 「New Task」タブ

アレイの新しいタスクを作成することができます。タスクをすぐに実行するか、スケジュールした時間に実行するかを選択できます。作成可能なタスクは「Verify」、「Verify with Fix」、「Clear」「Rebuild」です。それぞれのタスクに対する機能は以下とおりです。ZCRやHostRAIDの違いによって表示されないタスクもあります。

Verify: データの整合性のテストを行います。不整合が見つかっても、修復しません。

Verify with Fix: データの整合性のテストを行います。不整合が見つかった場合、修復します。

Clear: アレイ上のすべてのデータをクリアします。クリアを実施すると、クリア前のデータに回復することはできません。

> 重要 **Clearの実行中にシステムをシャットダウンしないでください。**

Rebuild: 手動でリビルドを実施します。

タスクの作成はアレイについてのみ可能です。チャネル、コントローラ、システムについてタスクを選択すると、関連するすべてのタスクが表示されます。

ただし、ここでスケジュールされたタスクは、一度実行されるとタスクから消去されます。冗長性のあるアレイには、定期的に週に1回程度、Verifyを行うことを推奨します。Verifyを定期的に行うには、専用のVerifyスケジューリングツールを使用します。詳しくは、「Verifyのスケジュールの設定」の説明を参照してください。

Verifyのスケジュール設定

Verifyスケジューリングツール(HrVerify)は、OSのcron機能を利用して動作します。

Verifyスケジューリングツール(HrVerify)は、ダウンロードしたファイルを使ってください。

1. HrVerifyコマンドの適用

① LinuxHrVerify.zipを任意のディレクトリにコピーする。

② #unzip LinuxHrVerify.zipで、解凍する。

③ HrVerifyコマンドが解凍されるので、/usr/bin配下にコピーする。

通常のコマンド起動で、使用可能です。

2. Verifyスケジュールの設定

コマンドのスケジュールは、crontabの設定をしてスケジューリングをします。

〔crontab設定〕

#crontab -e を、ターミナルから入力します。

コマンド入力後、エディタが表示されるので以下のようにスクリプトを編集します。
(以前に、登録した場合は前に登録されたイメージが出力されます)

スクリプトの記述:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

〔分〕〔時間〕〔日〕〔月〕〔曜日〕 /usr/bin/HrVerify all〔修復属性〕
```

上記の記述後、":"を押して"wq"で登録を終了してください。

〔パラメータ設定〕

〔分〕〔時間〕〔日〕〔月〕〔曜日〕は、数字で入力します。

指定しない項目は、"*"を入れることでスケジューリングされません。

[曜日]は、以下の数字で設定します。

"0"=日曜日,"1"=月曜日,"2"=火曜日,"3"=水曜日,"4"=木曜日,"5"=金曜日,"6"=土曜日

[修復属性]は、以下の"-Fix"または"-NoFix"を入力します。

-Fix: Verify with Fixを指定。データの不整合を検出した場合、修復を試みるモード。(推奨値)

-NoFix: Verify with No Fixを指定。データの不整合を検出しても修復しないモード。

(例1) 毎日02:00にVerifyを"Verify with Fix"のモードで自動実行する。

0 2 * * * /usr/bin/HrVerify all -Fix

(例2) 毎週水曜日の14:00にVerifyを"Verify with No Fix"のモードで自動実行する。

0 14 * * 3 /usr/bin/HrVerify all -NoFix

- [修復属性]に何も指定しなければ、デフォルトで"-Fix"が設定されます。
- この[修復属性]の各オプションはそれぞれ、前述したASMBEの「New Task」タブから設定できる"Verify with Fix"および"Verify"と同一の処理を行います。
- このVerifyスケジューリングツールによるVerify with FixおよびVerify with No Fix処理結果のログは、ASMBEログファイルを参照してください。

[設定されているパラメータの表示]

#crontab -l を、ターミナルから入力します。

[設定されているパラメータの削除]

#crontab -r を、ターミナルから入力します。

3. スケジュールの起動方法

上記、コマンドスケジュールの登録が終了した時点でcronを起動します。

[cronの起動]
#/etc/rc.d/init.d/crond start を、ターミナルから入力し起動します。

[cronの停止]
#/etc/rc.d/init.d/crond stop を、ターミナルから入力し停止します。

[cronの再起動]
#/etc/rc.d/init.d/crond restart を、ターミナルから入力し再起動します。

[cronの状態確認]
#/etc/rc.d/init.d/crond status を、ターミナルから入力し確認します。

システム負荷の低いタイミングを見計らって接続されるすべてのアレイを対象に定期的にVerifyを行うことを強く推奨します。Verifyを行うことにより、アクセス頻度の低いファイルや未使用領域の後発不良を早期に発見することができます。故障などによるハードディスク交換時のリビルドで、残りのハードディスクで後発不良が発見された場合、システムは復旧できないため、Verifyによる早期発見は、予防保守として非常に効果があります。定期的に実施することで、システムの安定した運用を保つ効果があり、週に1回は実施していただくことを強く推奨します。

通報監視について

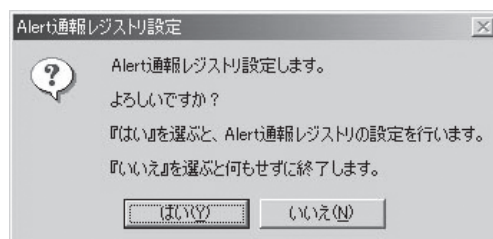
RAIDに関するイベント通報をESMPRO/AlertManager、ESMPRO/ServerManagerを使って監視を行うことができます(Windowsのみ使用可能)。

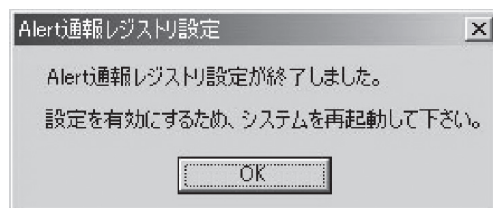
ESMPRO/ServerManagerインストール後、以下の手順で設定を行ってください。

1. 「ASMALRTJ.EXE」を起動する。

   「ASMALRTJ.EXE」は本装置に添付のバックアップCD-ROMの「¥nec¥Linux¥ASMBE¥HostRAID」にあります。

2. [はい]をクリックする。

   [いいえ]をクリックすると、設定をせずに終了します。

3. [OK]をクリックする。

4. システムを再起動する。

アラート通報メッセージと処置

ASMBEをインストールした直後は下記のメッセージを通報対象として設定します。この設定を変更する場合は、ESMPRO/ServerAgentの通報設定で定義し直してください。
下表のEventIDは10進数です。マネージャの列の「○」印はESMPRO/ServerManagerへの通知を示しています。「Alive」の列の「○」印はエクスプレス通報サービスへの通知を示しています。メッセージの%1などは埋め込み文字です。

Event ID	メッセージ	処　置	マネージャ	ALIVE
8204	Member is down on array "%1" [bus=%2, ch=%3, id=%4]	物理デバイスに障害がないか確認してください。適切な対処後、再度、リビルドを実施してください。	○	○
8205	Member is missing on array "%1"	物理デバイスやケーブルに障害がないか確認してください。	○	○
8206	Array "%1" is off-line; member failed	物理デバイスやケーブルに障害がないか確認してください。	○	○
8207	Array "%1" is off-line	物理デバイスやケーブルに障害がないか確認してください。	○	○
8210	Reconstruct started on array "%1"	なし	○	×
8211	Reconstruct completed on array "%1"	なし	○	×
8212	Reconstruct aborted on array "%1" due to I/O error	物理デバイスやケーブルに障害がないか確認してください。適切な対処後、再度、リビルドを実施してください。	○	○
8215	Verify aborted on array "%1" due to I/O error, no miscompares	物理デバイスやケーブルに障害がないか確認してください。適切な対処後、再度、リビルドを実施してください。	○	○
8217	Initialize aborted on array "%1" due to I/O error	物理デバイスやケーブルに障害がないか確認してください。	○	○
8225	Scheduled Verify deleted on array "%1"	対象のアレイがRAID 1または10か確認してください。物理デバイスがフェイル状態かを確認してください。SCSIエラーが報告されていないか確認してください。アレイの状態を確認してください。	○	○
8227	Array "%1" is critical	物理デバイスに障害がないか確認してください。適切な対処後、再度、リビルドを実施してください。	○	○
8237	Reconstruct failed to start on array "%1" due to I/O error	物理デバイスの接続状況や物理デバイス、ケーブルに障害がないか確認してください。障害を取り除いてからリビルドを実施してください。	○	○
8240	Array "%1" is now fault-tolerant	なし	○	×
8245	Update of array drives failed after Initialize	物理デバイスに障害がないか確認してください。適切な対処後、再度、initializeを実施してください。	○	○
8248	Scheduled Reconstruct failed to start on array "%1"	物理デバイスやケーブルに障害がないか確認してください。障害を取り除いてからリビルドを実施してください。他のリビルドが動作している場合はその完了を待ってください。	○	○
8249	Scheduled Verify failed to start on array "%1"	物理デバイスやケーブルに障害がないか確認してください。障害を取り除いてからリビルドを実施してください。	○	○
8259	Reconstruct is scheduled for array "%1"	なし	○	×
8270	Verify task failed to start on array "%1"	物理デバイスやケーブルに障害がないか確認してください。障害を取り除いてからリビルドを実施してください。	○	○

Event ID	メッセージ	処　置	マネージャ	ALIVE
8281	Dedicated spare [bus=%2, ch=%3, id=%4] not functional on array "%1"	物理デバイスを交換し、ホットスペアを作成してください。	○	○
8284	Array "%1" is still critical	ログをチェックし、問題が発生している物理デバイスの有無を確認してください。	○	○
8325	Verify aborted on array "%1" due to I/O error with %2 fixed miscompares	物理デバイスやケーブルに障害がないか確認してください。障害を取り除いてからリビルドを実施してください。	○	○
8336	Recovered error: SMART event received for array "%1" [bus=%2, ch=%3, id=%4 lun=%5]	物理デバイスが故障しています、該当物理デバイスを交換してください。	○	○
8337	Recovered error: SMART event received for device [bus=%1, ch=%2, id=%3 lun=%4]	物理デバイスが故障しています、該当物理デバイスを交換してください。	○	○
8340	I/O error aborted Verify array "%1", unfixed miscompares=%2	物理デバイスに障害がないか確認してください。適切な対処後、再度、リビルドを実施してください。	○	○
8363	Running Auto Reconstruct	なし	○	×
8365	Device [bus=%1, ch=%2, id=%3, lun=%4] is down	デバイスやディスク筐体をチェックし、故障の場合は交換してください。	○	○

アンインストール

重要

ASMBEのアンインストールはroot権限を持ったユーザーで行ってください。

1. インストール時に展開したファイルがあるディレクトリに移動し、ASMBE-RENICEツールのアンインストールを実行する。

   #rpm -e asmbe-renice

2. インストールコマンドを実行します。

   #./instasmbe -e

   インストールの最後に以下のメッセージが表示されていることを確認してください。

   Uninstallation Complete

   重要

   インストール時に展開したファイルを既に削除してしまっている場合は、再度、「インストール」の手順1～2を行ってください。

以上でASMBEのアンインストールは完了です。

7 故障かな?と思ったときは

「故障かな?」と思ったときは、修理を依頼する前にここで説明する内容について確認してください。また、この章では、修理を依頼する際の確認事項やNEC、およびNECが認定する保守サービス会社が提供するさまざまなサービスについても説明があります。

日常の保守

本装置を常にベストな状態でお使いになるために、ここで説明する確認や保守を定期的に行ってください。万一、異常が見られた場合は、無理な操作をせずに保守サービス会社に保守を依頼してください。

アラートの確認

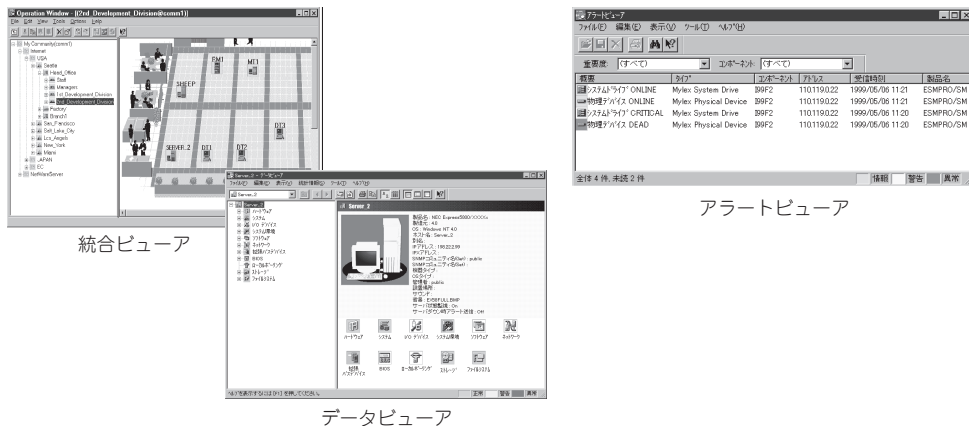
システムの運用中は、ESMPROで障害状況を監視してください。

管理コンピュータ上のESMPRO/ServerManagerにアラートが通報されていないか、常に注意するよう心がけてください。ESMPRO/ServerManagerの「統合ビューア」、「データビューア」、「アラートビューア」でアラートが通報されていないかチェックしてください。

ESMPROでチェックする画面

統合ビューア

データビューア

アラートビューア

また、ファイアウォール機能のアラートについては、Management Consoleの「ファイアウォール」メニューから「アラート表示」をクリックして表示される画面で確認することができます。 4章の「情報表示」—「ログ・アラート表示」を参照してください。

ステータスランプの確認

本体の電源をONにした後、およびシャットダウンをして電源をOFFにする前に、本体前面にあるランプの表示を確認してください。ランプの機能と表示の内容については2章を参照してください。万一、装置の異常を示す表示が確認された場合は、保守サービス会社に連絡して保守を依頼してください。

バックアップ

システムにインストールしたシステム基本情報とセキュリティポリシーは必ずバックアップをとってください。
再インストールの際にリストアすることにより、再インストール前と同じ状態にセットアップすることができます。バックアップ/リストアについては4章を参照してください。

クリーニング

本装置を良い状態に保つために定期的にクリーニングしてください。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **自分で分解・修理・改造はしない**
- **プラグを差し込んだまま取り扱わない**

本体のクリーニング

本体の外観の汚れは、柔らかい乾いた布で汚れを拭き取ってください。汚れが落ちにくいときは、次のような方法できれいになります。

重要

- **シンナー、ベンジンなどの揮発性の溶剤は使わないでください。材質のいたみや変色の原因になります。**
- **コンセント、ケーブル、本体背面のコネクタ、本体内部は絶対に水などでぬらさないでください。**

1. 本体の電源がOFF(POWERランプ消灯)になっていることを確認する。
2. 本体の電源コードをコンセントから抜く。
3. 電源コードの電源プラグ部分についているほこりを乾いた布でふき取る。
4. 中性洗剤をぬるま湯または水で薄めて柔らかい布を浸し、よく絞る。
5. 本体の汚れた部分を手順4の布で少し強めにこすって汚れを取る。
6. 真水でぬらしてよく絞った布でもう一度ふく。
7. 乾いた布でふく。
8. 乾いた布で背面にある排気口に付着しているほこりをふき取る。

CD-ROMのクリーニング

CD-ROMにほこりがついていたり、トレーにほこりがたまっていたりするとデータを正しく読み取れません。次の手順に従って定期的にトレー、CD-ROMのクリーニングを行います。

1. 本体の電源がON(POWERランプ点灯)になっていることを確認する。
2. CD-ROMドライブ前面のCDトレーイジェクトボタンを押す。

   トレーがCD-ROMドライブから出てきます。
3. CD-ROMを軽く持ちながらトレーから取り出す。

   重要

   CD-ROMの信号面に手が触れないよう注意してください。
4. トレー上のほこりを乾いた柔らかい布でふき取る。

   重要

   CD-ROMドライブのレンズをクリーニングしないでください。レンズが傷ついて誤動作の原因となります。
5. トレーをCD-ROMドライブに戻す。
6. CD-ROMの信号面を乾いた柔らかい布でふく。

   重要

   CD-ROMは、中心から外側に向けてふいてください。クリーナをお使いになるときは、CD-ROM専用のクリーナであることをお確かめください。レコード用のスプレー、クリーナ、ベンジン、シンナーを使用すると、ディスクの内容が読めなくなったり、本体にそのディスクをセットした結果、故障したりするおそれがあります。

障害時の対処

「故障かな？」と思ったときは、ここで説明する内容について確認してください。該当することがらがある場合は、説明に従って正しく対処してください。

障害箇所の切り分け

万一、障害が発生した場合は、ESMPRO/ServerManagerを使って障害の発生箇所を確認し、障害がハードウェアによるものかソフトウェアによるものかを判断します。

障害発生箇所や内容の確認ができたら、故障した部品の交換やシステム復旧などの処置を行います。障害がハードウェア要因によるものかソフトウェア要因によるものかを判断するには、ESMPRO/ServerManagerが便利です。ハードウェアによる障害をさらに切り分けるには、「EXPRESSBUILDER（SE）」の「システム診断」をご利用ください。システム診断については5章をご覧ください。また、4章の「情報表示」－「ログ・アラート表示」で説明したインタフェースを利用して、アラート情報を出力するファイルの内容を参照し、障害を起こしているモジュール名を取得してください。

エラーメッセージ　- 電源ON後のビープ音 -

電源ON直後に始まるPower On Self-Test（POST）中にエラーを検出すると一連のビープ音でエラーが発生したことを通知します。エラーはビープ音のいくつかの音の組み合わせでその内容を通知します。
たとえば、ビープ音が1回、連続して3回、1回、1回の組み合わせで鳴った（ビープコード: 1-3-1-1）ときはDRAMリフレッシュテストエラーが起きたことを示します。

次にビープコードとその意味を示します。エラーが起きたときはお買い求めの販売店または保守サービス会社に連絡して保守を依頼してください。

ビープコード	意　味	対処方法
3-3-(繰り返し)	ROMチェックサムエラー	保守サービス会社に連絡してマザーボードを交換してください。
1-2-2-3	ROMチェックサムエラー	
1-3-1-1	DRAMリフレッシュテストエラー	DIMMの取り付け状態を確認してください。それでも直らない場合は保守サービス会社に連絡してDIMMまたはマザーボードを交換してください。
1-3-1-3	キーボードコントローラテストエラー	キーボードを接続し直してください。それでも直らない場合は保守サービス会社に連絡してマザーボードを交換してください。
1-3-3-1	メモリを検出できない メモリの容量チェック中のエラー	DIMMの取り付け状態を確認してください。それでも直らない場合は保守サービス会社に連絡してDIMM、またはマザーボードを交換してください。
1-3-4-1	DRAMアドレスエラー	
1-3-4-3	DRAMテスト Low Byteエラー	
1-4-1-1	DRAMテスト High Byteエラー	
1-5-1-1	CPUの起動エラー	保守サービス会社に連絡してマザーボードを交換してください。
1-5-2-1	CPUが搭載されていない	保守サービス会社に連絡してCPUまたはマザーボードを交換してください。
1-5-4-4	電源異常	保守サービス会社に連絡してマザーボードを交換してください。
2-1-2-3	BIOS ROMコピーライトテストエラー	
2-2-3-1	不正割り込みテストエラー	
1-2	オプションROM初期化エラー	SETUPの設定を確認してください。また、増設したPCIボードのオプション ROMの展開が表示されない場合は、PCIボードの取り付け状態を確認してください。 それでも直らない場合は保守サービス会社に連絡して、増設したPCIボード、またはマザーボードを交換してください。

ピープコード「1-5-4-2」の鳴動は停電や瞬断などによりAC電源の供給が遮断され、システムの再起動が行われたことを通知するものです。異常ではありません。

トラブルシューティング

装置が思うように動作しない場合は修理に出す前に次のチェックリストの内容に従ってチェックしてください。リストにある症状に当てはまる項目があるときは、その後の確認、処理に従ってください。
それでも正常に動作しない場合は保守サービス会社に連絡してください。

装置が思うように動作しない場合は修理に出す前に次のチェックリストの内容に従ってチェックしてください。リストにある症状に当てはまる項目があるときは、その後の確認、処理に従ってください。
それでも正常に動作しない場合は保守サービス会社に連絡してください。

本体について

OSのシステムエラーが発生した

→ システムにアクセスできず、本体のディスクアクセスが長く続く場合はシステムエラー(パニック)が発生している可能性があります。 パニック発生時にはダンプが採取され、その後自動的にシステムが再起動されます。 また、システム再起動時にシステムエラーの発生がESMPRO/ServerAgentにより検出されます。

システムエラーの障害調査には/var/log/vmdump配下のファイルすべてと/var/log/messagesファイル、およびksyms -aコマンドを実行して、その結果をファイルに出力したものを採取する必要があります。 採取の方法は、管理コンピュータ(コンソール)から障害発生サーバにログインし、障害発生サーバからFTPで情報を採取します。情報の採取後は/var/log/vmdump配下のファイルはすべて削除可能です。削除しない場合、システムエラー(パニック)が発生するたび、ダンプファイルが追加作成されます(前回のダンプファイルは上書きされません)。

本体の電源が自動的にOFFになった

□ 装置の温度が高くなりすぎた可能性があります。通気が妨げられていないか確認し、装置の温度が下がってから再起動してください。それでも電源がOFFになる場合は、保守サービス会社に連絡してください。

起動完了ビープ音が定期的に何度も鳴る

□ 一度電源をOFFにして、再起動してみてください。それでも、起動完了ビープ音が定期的に鳴る場合は保守サービス会社に連絡してください。

管理コンピュータに画面が表示されない

□ ハードウェア構成情報を正しく設定していますか?
→ 添付の「EXPRESSBUILDER(SE)CD-ROM」を使ってシステムを起動してBIOSの設定値をリロードしてみてください(317ページの「ヒント」参照)。それでも表示できない場合は、保守サービス会社に連絡してください。

フロッピーディスクにアクセス(読み込み、または書き込みが)できない

□ フロッピーディスクをフロッピーディスクドライブにセットしていますか?
→ フロッピーディスクドライブに「カチッ」と音がするまで確実に差し込んでください。

□ 書き込み禁止にしていませんか?
→ フロッピーディスクのライトプロテクトスイッチを「書き込み可」にセットしてください。

CD-ROMにアクセスできない

□ CD-ROMドライブのトレーに確実にセットしていますか?
→ トレーに確実にセットされていることを確認してください。

CD-ROMドライブの回転音が大きい

□ いったん、CD-ROMを取り出し、再度CD-ROMをセットし直してください。
→ CD-ROMドライブのオートバランス機構を再度機能させることで、回転音をおさえます。

Management Consoleについて

Management Consoleと接続できない

→ URLが正しいかを確認してください。

→ リモートメンテナンスの操作可能ホストとして登録されている管理クライアントから接続しているかを確認してください。

→ 入力した管理者アカウント名、パスワードが正しいか確認してください。

→ サーバ公開ルールの設定において、Express5800/SG300自身のインタフェースを外部公開IPアドレスとして指定し、ポートの指定をしない設定にした場合にManagement Consoleと接続できなくなります。

このように、ルールの設定誤りによりManagement Consoleと接続できなくなった場合は、次の手順により復旧させてください。

1. シリアルコンソールからrootユーザでログインする。
2. 次のコマンドを実行する。

```
sgfwclear
```

   これにより登録されているルールがすべて無効化されます。

3. Management Consoleに接続し、ルールを修正する。
4. 「編集結果を適用」ボタンによりルールを適用する。

ユーザ認証について

ユーザログイン画面が表示されない

→ URLが正しいかを確認してください。

→ かんたん設定ウィザードまたは詳細設定メニューの認証設定において、ユーザ認証を行うためのチェックボックスにチェックが入っていることを確認してください。ユーザ認証の利用を選択しておく必要があります。

→ ルールによってHTTP通信を拒否していないかを確認してください。

ユーザ認証に失敗する

→ 入力したユーザID、パスワードが正しいか確認してください。

→ ユーザアカウントがロックアウトされていませんか？ロックアウトを解除してください。

EXPRESSBUILDER(SE)について

EXPRESSBUILDER(SE)CD-ROMから本装置を起動できない

□ システムBIOSの起動デバイスが正しく設定されていない可能性があります。正しく設定できているか確認してみてください。

□ POSTを実行中にEXPRESSBUILDER(SE) CD-ROMをセットし、再起動しないとエラーメッセージが表示されたり、OSが起動したりします。

EXPRESSBUILDER(SE)を実行中、何らかの障害が発生すると、以下のようなメッセージが表示されます。メッセージ内容を記録して保守サービス会社に連絡してください。

この他にもシステム診断を実行したときに障害を検出するとエラーメッセージが表示されます。表示されたメッセージ内容を記録して保守サービス会社までご連絡ください。

メッセージ	原因と処理方法
本プログラムの動作対象マシンではありません。	EXPRESSBUILDER（SE）の対象マシンではありません。対象マシンで実行してください。
NvRAMへのアクセスに失敗しました。	不揮発性メモリ(NVRAM)にアクセスできません。
ハードディスクへの アクセスに失敗しました。	ハードディスクが接続されていないか、ハードディスク が異常です。ハードディスクが正常に接続されていることを確認して ください。

メインメニューが文字化けしている

□ コンソールのモードが実際のコンソールと異なっている可能性があります。
LAN接続またはダイレクト接続(COM B)された管理コンピュータから実行してください。

マスターコントロールメニューについて

オンラインドキュメントが読めない

□ Adobe Acrobat Readerが正しくインストールされていますか？
→ オンラインドキュメントの一部は、PDF形式で提供されています。あらかじめAdobe Acrobat Reader(Version 4.05以上)をご使用のオペレーティングシステムへインストールしておいてください。なお、Adobe Acrobat Readerは、「EXPRESSBUILDER（SE） CD-ROM」からインストールすることができます。マスターコントロールメニューを起動後、「ソフトウェアのセットアップ」の「Adobe Acrobat Reader」を選択してください。

□ 使用しているOSは、Windows XP Service Pack2（SP2）ですか？
→ SP2にてオンラインドキュメントを表示しようとすると、ブラウザ上に以下のような情報バーが表示されることがあります。

「セキュリティ保護のため、コンピュータにアクセスできるアクティブコンテンツは表示されないよう、Internet Explorerで制限されています。オプションを表示するには、ここをクリックしてください...」

この場合、以下の手順にてドキュメントを表示させてください。

1. 情報バーをクリックする。

   ショートカットメニューが現れます。

2. ショートカットメニューから、「ブロックされているコンテンツを許可」を選択する。

   「セキュリティの警告」ダイアログボックスが表示されます

3. ダイアログボックスにて「はい」を選択する。

オンラインドキュメントの画像が見にくい

□ ご使用のディスプレイは、256色以上の表示になっていますか？
→ ディスプレイの設定が256色未満の場合は、画像が見にくくなります。256色以上の表示ができる環境で実行してください。

マスターコントロールメニューが表示されない

□ ご使用のシステムは、Windows NT 4.0以降、またはWindows 95以降ですか？
→ 本プログラムは、Windows 95以降またはWindows NT 4.0 以降のオペレーティングシステム上にて動作させてください。

□ <Shift>キーを押していませんか？
→ <Shift>キーを押しながらCD-ROMをセットしますと、Autorun機能がキャンセルされます。

□ システムの状態は問題ありませんか？
→ システムのレジストリ設定やCD-ROMをセットするタイミングによってはメニューが起動しない場合があります。そのような場合は、CD-ROMの¥MC¥1ST.EXEをエクスプローラ等から実行してください。

「This program requires Windows Japanese version」というメッセージが表示される

□ ご使用の環境は正しいですか？

→ 本製品は、日本語版Windows専用です。オペレーティングシステムが英語バージョンの場合、プログラムは起動できませんので、日本語バージョンのオペレーティングシステムにて動作させてください。

メニュー項目がグレイアウトされている

□ ご使用の環境は正しいですか？

→ 実行するソフトウェアによっては、管理者権限が必要だったり、本装置上で動作することが必要だったりします。適切な環境にて実行するようにしてください。

ESMPROについて

画面が文字化けしている

→ シリアル接続の管理クライアントから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
#export LANG=C
```

ESMPROで思うように監視できない・動作しない

→ 本体に添付のCD-ROMにあるオンラインドキュメントを参照してください。本体にインストールされているESMPRO/ServerAgentについては、添付の「バックアップCD-ROM:/nec/Linux/esmpro.sa/doc」を参照してください。ESMPRO/ServerManagerについては、「EXPRESSBUILDER（SE） CD-ROM」内にあります。「EXPRESSBUILDER（SE） CD-ROM」をWindowsマシンにセットすると自動的にメニューが表示されます。メニューからオンラインドキュメントを選択してください。

FAQ

一般的に多く寄せられる疑問や質問に関する回答集です。参考にしてください。

GUI関連

Q: Express5800/FW300、FW500に添付されているGUIクライアントでExpress5800/SG300 に接続できますか？

A: 接続できません。ウェブブラウザを使用してExpress5800/SG300のManagement Consoleに接続してください。

Q: 推奨のウェブブラウザは？

A: Microsoft Internet Explorer 6.0 SP1（日本語版・Windows版）を推奨します。

NAT

Q: NATは使用できますか？

A: 使用できます。サーバ公開ルールの設定を参照してください。

認証

Q: ユーザーごとに認証を設けてアクセス制限をかけられますか？

A: 可能です。ユーザ認証の設定を参照してください。

ライセンス関連

Q: ノード数によるライセンスの違いがありますか？

A: ノード数によってライセンスが異なることはありません。

Q: Express5800/SG300のIPアドレスを変更できますか？

A: IPアドレス変更の申請を行い、変更後のIPアドレス用のライセンスキーを入手する必要があります。また、IPアドレス変更の申請にはサポートサービス製品を購入している必要があります。

その他

Q: Express5800/SG300に他のアプリケーションサーバを同居させることはできますか？

A: セキュリティの観点から同居させないようにしてください。

Q: 外部インタフェースを複数持つことができますか？

A: できません。

移動と保管

本体を移動・保管するときは次の手順に従ってください。

警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 自分で分解・修理・改造はしない
- リチウム電池を取り外さない
- プラグを差し込んだまま取り扱わない

注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 中途半端に取り付けない
- 落下注意
- 装置を引き出した状態にしない
- カバーを外したまま取り付けない
- 指を挟まない
- 高温注意
- ラックが不安定な状態でデバイスをラックから引き出さない
- 複数台のデバイスをラックから引き出した状態にしない

重要

- フロアのレイアウト変更など大掛かりな作業の場合はお買い上げの販売店または保守サービス会社に連絡してください。
- ハードディスクドライブに保存されている大切なデータはバックアップをとっておいてください。
- 本装置にはハードディスクドライブが内蔵されています。ハードディスクドライブに衝撃を与えないように注意して本体を移動させてください。
- 再度、運用する際、内蔵機器や本体を正しく動作させるためにも室温を保てる場所に保管することをお勧めします。装置を保管する場合は、保管環境条件(温度:-10~55℃、湿度:20~80%)を守って保管してください(ただし、結露しないこと)。

1. フロッピーディスクやCD-ROMをセットしている場合は本体から取り出す。
2. クライアントマシンのWebブラウザからシステムのシャットダウン処理をして電源をOFF(POWERランプ消灯)にする。
3. 本体の電源プラグをコンセントから抜く。

4. 本体に接続しているケーブルをすべて取り外す。

5. 本体をラックに搭載している場合は、2章を参照して本体をラックから取り出す。

   なるべく複数名で行うことをお勧めします。

6. 本体に傷がついたり、衝撃や振動を受けたりしないようしっかりと梱包する。

重要

輸送後や保管後、装置を再び運用する場合は、運用の前にシステム時計の確認・調整をしてください。システム時計を調整しても時間の経過と共に著しい遅れや進みが生じる場合は、お買い求めの販売店、または保守サービス会社に保守を依頼してください。本装置、および、内蔵型のオプション機器は、寒い場所から暖かい場所に急に持ち込むと結露が発生し、そのまま使用すると誤動作や故障の原因となります。装置の移動後や保管後、再び運用する場合は、使用環境に十分なじませてからお使いください。

ユーザーサポート

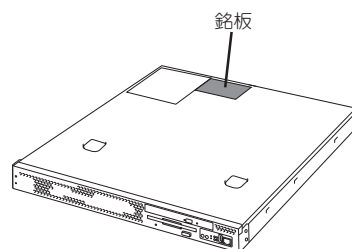
アフターサービスをお受けになる前に、保証およびサービスの内容について確認してください。

保証について

本装置には『保証書』が添付されています。『保証書』は販売店で所定事項を記入してお渡ししますので、記載内容を確認のうえ、大切に保管してください。保証期間中に故障が発生した場合は、『保証書』の記載内容にもとづき無償修理いたします。詳しくは『保証書』およびこの後の「保守サービスについて」をご覧ください。

保証期間後の修理についてはお買い求めの販売店、もよりのNECまたは保守サービス会社に連絡してください。

重要

- NEC製以外(サードパーティ)の製品、またはNECが認定していない装置やインタフェースケーブルを使用したために起きた本装置の故障については、その責任を負いかねますのでご了承ください。
- 本体の上面に、製品の形式、SERIAL No.(号機番号)、定格、製造業者名、製造国が明記された銘板が貼ってあります。販売店にお問い合わせする際にこの内容をお伝えください。また銘板の号機番号と保証書の保証番号が一致していませんと、装置が保証期間内に故障した場合でも、保証を受けられないことがありますのでご確認ください。万一違う場合は、お買い求めの販売店にご連絡ください。

修理に出される前に

「故障かな？」と思ったら、以下の手順を行ってください。

① 電源コードおよび他の装置と接続しているケーブルが正しく接続されていることを確認します。

② 「障害時の対処(423ページ)」を参照してください。該当する症状があれば記載されている処理を行ってください。

③ 本装置を操作するために必要となるソフトウェアが正しくインストールされていることを確認します。

以上の処理を行ってもなお異常があるときは、無理な操作をせず、お買い求めの販売店、最寄りのNECまたは保守サービス会社にご連絡ください。その際に本体のランプの表示や管理コンピュータのディスプレイ装置のアラーム表示もご確認ください。故障時のランプやディスプレイによるアラーム表示は修理の際の有用な情報となることがあります。保守サービス会社の連絡先については、付録D「保守サービス会社網一覧」をご覧ください。
なお、保証期間中の修理は必ず保証書を添えてお申し込みください。

重要

この製品は日本国内仕様のため、NECの海外拠点で修理することはできません。ご了承ください。

修理に出される時は

修理に出される時は次のものを用意してください。

□ 保証書

□ クライアントマシンのWebブラウザに表示されたメッセージのメモ

□ 障害情報(ネットワークの接続形態や障害が起きたときの状況)

□ 本体・周辺機器の記録

補修用部品について

本装置の補修用部品の最低保有期間は、製造打ち切り後5年です。

保守サポート/保守サービスについて

ソフトウェアに関するサポート

ソフトウェアに関するサポートについては1章の「Express5800/SG300について」で記載している「ソフトウェアサポートサービス」を参照してください。

ソフトウェア以外に関するサポート

保守サービスはNECの保守サービス会社、およびNECが認定した保守サービス会社によってのみ実施されますので、純正部品の使用はもちろんのこと、技術力においてもご安心の上、ご都合に合わせてご利用いただけます。
なお、お客様が保守サービスをお受けになる際のご相談は、弊社営業担当または代理店で承っておりますのでご利用ください。保守サービスは、お客様に合わせて2種類用意しております。

保守サービスメニュー

契約保守サービス	お客様の障害コールにより優先的に技術者を派遣し、修理にあたります。 この保守方式は、装置に応じた一定料金で保守サービスを実施させていただくもので、お客様との間に維持保守契約を結ばせていただきます。 さまざまな保守サービスを用意しています。詳しくはこの後の説明をご覧ください。
未契約修理	お客様の障害コールにより、技術者を派遣し、修理にあたります。保守または修理料金はその都度精算する方式で、作業の内容によって異なります。

NECでは、お客様に合わせて以下の契約保守サービスを用意しております。

- **サービスを受けるためには事前の契約が必要です。**
- **サービス料金は契約する日数/時間帯により異なります。**

ハードウェアメンテナンスサービス

維持保守

定期的な点検により障害を予防します。(定期予防保守)
また、万一障害発生時には保守技術者がすみやかに修復します。(緊急障害復旧)

出張修理

障害発生時、保守技術者が出張して修理します。(緊急障害復旧)

エクスプレス通報サービス

ご契約の期間中、お客様の本体を監視し、障害(アレイディスク縮退、メモリ縮退、温度異常等)が発生した際に保守拠点からお客様に連絡します。お客様への連絡時間帯は、月曜日～金曜日　午前9:00～午後5:00です。

「ハードウェアメンテナンスサービス」または「マルチベンダH/W統括サービス」を契約されたお客様は無償でこの保守サービスをご利用することができます。
(お申し込みには「申込書」が別途必要です。販売店、弊社営業担当にお申し付けください。)

オプションサービス

下記のオプションサービスもございますのでご利用ください。

マルチベンダH/W統括サービス

マルチベンダ製品(本製品+SI仕入製品*)で構成されるクライアント・サーバ・システムに対し、下記の形態による修理を行います。

維持保守形態	定期予防保守と、障害発生機器の切り分け、緊急障害復旧を行います。
出張保守形態	障害発生機器の切り分け、緊急障害復旧を行います。
引取り保守形態	障害発生機器の切り分け、取外し、引取り、持帰り、調査、修理をし、完了後に取付け、動作確認、修理内容報告、引渡しを行います。
預り保守形態	お客様が送付された故障品を修理し、完了後にご返送します。

*　SI仕入製品とは・・・
NECが他社から仕入れ、責任をもってお客様に納入させていただく他社製品のことです。

LANマルチベンダ保守サービス

他社製品を含むマルチベンダで構成されるLAN機器(ルータ・HUB・ブリッジなど)について、障害原因の切り分けとお客様が選んだ保守方式による障害修復を行います。クライアントおよびサーバは、本メニュー対象外です。
NEC製のLAN機器は出張修理を行います。
他社製品のLAN機器についても、シングルウインドウでその障害修復(センドバック、予備機保守など、お客様が選んだ保守方式による)までをフォローします。

LAN・ネットワーク監視サービス

お客様が準備したLAN・ネットワーク監視装置を使用し、INS回線経由で監視します。サービス内容はネットワークノードの障害監視から、性能監視、構成監視まであります。サービス日時は、24時間・365日まで9パターンから選択できます。監視の結果は毎月報告書を発行します。修理はハードウェアメンテナンスサービスで対応します。

情報サービスについて

本製品に関するご質問・ご相談は「ファーストコンタクトセンター」でお受けしています。
※　電話番号のかけまちがいが増えております。番号をよくお確かめの上、おかけください。

ファーストコンタクトセンター　TEL. 03-3455-5800（代表）

受付時間／9:00〜12:00、13:00〜17:00　月曜日〜金曜日（祝祭日を除く）

お客様の装置本体を監視し、障害が発生した際に保守拠点からお客様に連絡する「エクスプレス通報サービス」の申し込みに関するご質問・ご相談は「エクスプレス受付センター」でお受けしています。
※　電話番号のかけまちがいが増えております。番号をよくお確かめの上、おかけください。

エクスプレス受付センター　TEL. 0120-22-3042
受付時間／9:00〜17:00　月曜日〜金曜日（祝祭日を除く）

インターネットでも情報を提供しています。

http://nec8.com/

『NEC 8番街』：製品情報、Q&Aなど最新Express情報満載！

http://club.express.nec.co.jp/

『Club Express』：『Club Express会員』への登録をご案内しています。Express5800シリーズをご利用になる上で役立つ情報サービスの詳細をご紹介しています。

http://www.fielding.co.jp/

NECフィールディング（株）ホームページ：メンテナンス、ソリューション、用品、施設工事などの情報をご紹介しています。

付録A　仕　様

型　名		Express5800/SG300b
		N8100-1017
プロセッサ	タイプ	Intel® Pentium® 4 processor
	動作周波数	3EGHz
	キャッシュメモリ	1MB（二次）
	標準	1個
	最大	1個
チップセット		Intel E7210
メモリ	標準	256MB
	最大	4GB
	誤り検出・訂正機能	あり（ECC）
ハードディスク	標準	80GB×1
	最大	80GB×2
インタフェース	SCSI	なし
	LAN	10BASE-T/100BASE-TX/1000BASE-TX×2チャネル 1000BASE-T×2チャネル
	IDE	Ultra ATA100×2チャネル SATA150×2チャネル
ディスクアレイ		標準装備（SATA）
フロッピーディスクドライブ		3.5インチ×1（1.44MB,720KB対応）
CD-ROMドライブ		10〜24倍速以上（ATAPI、トレーロード式）
デバイスベイ	5.25インチ	1スロット（CD-ROM用）
	3.5インチ	2スロット（1スロット占有）
拡張スロット（PCI）		2スロット（1スロット占有）
外部用インタフェース	シリアル	D-sub 9-pin（RS-232C規格準拠）×2
	ネットワーク	RJ-45×2
筐体デザイン		ラックマウント（1U）
外形寸法		427.5mm（幅）×501mm*（奥行き）×42.6mm（高さ）　＊ フロントベゼル取り付け時は547mm
質量（最大）		11kg
電源		AC100V±10%, 50/60Hz±1Hz
消費電力		280VA、270W
環境条件	動作時	温度:10〜35℃、湿度:20〜80%（ただし、結露しないこと）
	保管時	温度: -10〜55℃、湿度:20〜80%（ただし、結露しないこと）

付録B　二重化機能のログメッセージ

二重化機能では動作の履歴や異常の検出をシステムログ(syslog)に出力します。出力するメッセージとその説明、対処方法は以下のようになります。

イベントID	イベント分類	メッセージ	説明	対処
IDM001	情報	Starting.....	クラスタシステムの起動中です。	―
IDM001	情報	Shutting down.....	クラスタシステムの終了中です。	―
IDM003	情報	stopping all process.....	内部プロセスが異常終了したため、全プロセスを停止します。	システムを再起動してください。
IDM004	情報	Halting system.....	内部プロセスが異常終了したため、システムを停止します。	
IDM005	情報	Rebooting system.....	内部プロセスが異常終了したため、システムを再起動します。	―
IDM006	情報	Restarting main process.....	main プロセスが異常終了したため、main プロセスを再起動します。	―
IDM007	情報	Restarting send process.....	sendプロセスが異常終了したため、sendプロセスを再起動します。	―
IDM008	情報	Restarting recv process.....	recvプロセスが異常終了したため、recvプロセスを再起動します。	―
IDM009	情報	Auto startup is disabled.	自動起動に設定されていません。	基本設定ツール（fwsetup）で自動起動するように設定してください。
EDM001	異常	Main process abnormal exit.....	内部異常を検出したため、mainプロセスが異常終了しました。	引き続きRestarting main processが出力されれば自動リカバリに成功しています。
EDM002	異常	Send process abnormal exit.....	内部異常を検出したため、HB送信プロセスが異常終了しました。	引き続きRestarting send processが出力されれば自動リカバリに成功しています。
EDM003	異常	Recv process abnormal exit.....	内部異常を検出したため、HB受信プロセスが異常終了しました。	引き続きRestarting recv processが出力されれば自動リカバリに成功しています。
EDM007	異常	Configuration file is invailed.	設定がされていないか、設定の情報が不正です。	基本設定ツール（fwsetup）で設定内容を確認してください。
EDM008	異常	Critical error occured	致命的な異常が発生しました。	システムを再起動してください。
IGM001	情報	%1 start.	業務%1が起動しました。Firewall機能が起動された側のサーバで出力されます。	―
IGM002	情報	%1 stop.	業務%1が停止しました。Firewall機能が停止された側のサーバで出力されます。	―
IGM003	情報	%1 failover start.	業務%1のフェイルオーバー処理を開始します。	―
IGM004	情報	%1 failback start.	業務%1のフェイルバック処理を開始します。	―
EGM001	異常	%1 start failed.	業務%1が起動に失敗しました。	リソースに異常がなければ、システムを再起動してください。
EGM002	異常	%1 stop failed.	業務%1が停止に失敗しました。	リソースに異常がなければ、システムを再起動してください。

イベントID	イベント分類	メッセージ	説明	対処
EGM003	異常	%1(%2) error. stop %2.	リソース%1に異常が発生しました。再起動できなかったため、業務%2を停止します。	%1が、 - FIPの場合、[ERFxxx]の項を参照してください。 - EXECの場合、[EREｘxx]の項を参照してください。 - IPWの場合、[ERIxxx]の項を参照してください。 - PARPの場合、[ERPxxx]の項を参照してください。
EGM004	異常	%1(%2) error. failover %2.	リソース%1に異常が発生しました。業務%2をフェイルオーバします。	%1が、 - FIPの場合、[ERFxxx]の項を参照してください。 - EXECの場合、[EREｘxx]の項を参照してください。 - IPWの場合、[ERIxxx]の項を参照してください。 - PARPの場合、[ERPxxx]の項を参照してください。
IMN001	情報	all node wake up.	起動待ち合わせ時間内に、全サーバが起動しました。	—
IMN002	情報	wait timeout.	起動待ち合わせがタイムアウトしました。	待機系サーバでFirewall機能が動作している可能性があります。運用系サーバが起動してきたら、必要に応じてFirewall機能を運用系サーバに移動してください。
IMN003	警告	%1 down.	サーバ%1がダウンしました。	サーバ%1の障害を取り除いてください。引き続きIGM001のイベントが登録されていれば、フェイルオーバが成功しています。
IMN004	情報	%1 up.	サーバ%1が起動しました。	—
IMN010	情報	ignore stop message from %1.	サーバ%1からの停止メッセージを無視しました。	—
EMN001	異常	boot fail. stop.	内部異常のためmainプロセスの起動に失敗しました。	システムを再起動してください。
IRF001	情報	%1(%2):%3/%4 turned available.	業務%1のFIPリソース%2(IPアドレス%3／ネットマスク%4)の活性に成功しました。(異常状態からの復帰時のみ出力)	—
ERF001	異常	%1(%2):%3/%4 can’t enable.	業務%1のFIPリソース%2(IPアドレス%3／ネットマスク%4)の活性に失敗しました。	既に使用されているIPアドレスとFIPが重複している可能性があります。確認してください。
IRE001	情報	%1(%2):%3 turned executable.	業務%1のEXECリソース%2(実行パス%3)の実行に成功しました。(異常状態からの復帰時のみ出力)	—
ERE001	異常	%1(%2):%3 can’t execute.	業務%1のEXECリソース%2(実行パス%3)の実行に失敗しました。	/opt/necfws/bin/ckcstat /opt/necfws/bin/ckfwalive のパスが存在していることを確認してください。
ERE002	異常	%1(%2):%3 is disappear.	業務%1のEXECリソース%2(実行パス%3)の監視で異常が発生しました。	Firewall 機能に異常が発生した可能性があります。VPN-1/FireWall-1 の管理GUIで状況を確認してください。
IRI001	情報	%1(%2):%3 turned reachable.	業務%1のIPWリソース%2(監視アドレス%3)との通信が復帰しました。	—
ERI001	異常	%1(%2):%3 can’t reach.	業務%1のIPWリソース%2(監視アドレス%3)の監視で異常が発生しました。	監視対象のネットワークを確認してください。
IRP001	情報	%1(%2):%3 turned available.	業務%1のPARPリソース%2(IPアドレス%3)の活性に成功しました。(異常状態からの復帰時のみ出力)	—
ERP001	異常	%1(%2):%3 can’t enable.	業務%1のFIPリソース%2(IPアドレス%3の活性に失敗しました。	既に使用されているIPアドレスとPARPアドレスが重複している可能性があります。確認してください。

付録C　保守サービス会社網一覧

NEC Express5800シリーズ、および関連製品のアフターサービスは、お買い上げのNEC販売店、最寄りのNEC、またはNECフィールディング株式会社までお問い合わせください。下記にNECフィールディングのサービス拠点所在地一覧を示します。
（受付時間：AM9:00～PM5:00　土曜日、日曜日、祝祭日を除く）
次のホームページにも最新の情報が記載されています。

http://www.fielding.co.jp/

このほか、NEC販売店のサービス網がございます。お買い上げの販売店にお問い合わせください。
トラブルなどについてのお問い合わせは下記までご連絡ください（電話番号のおかけ間違いにご注意ください）。その他のお問い合わせについては、下表を参照してください。

電話番号　0120-911-111

2004年5月現在

都道府県名	拠点名	電話番号	郵便番号	所在地
北海道	札幌支店	011-221-3705	060-0042	札幌市中央区大通西4-1　新大通ビル9F
	新札幌支店	011-894-1131	004-0041	札幌市厚別区大谷地東4-2-20　第二西村ビル1F
	釧路営業所	0154-43-2361	085-0847	釧路市大町1-1-1　道東経済センタービル7F
	旭川支店	0166-24-2098	070-0033	旭川市三条通9丁目左1号　明治生命旭川ビル1F
	オホーツク営業所	0157-25-7520	090-0024	北見市北四条東3-1-1　富士火災北見ビル3F
	苫小牧営業所	0144-36-3846	053-0027	苫小牧市王子町3-2-23　朝日生命苫小牧ビル2F
	室蘭営業所	0143-46-3180	050-0083	室蘭市東町2-24-4　石井第5ビル3F
	函館支店	0138-54-5642	040-0001	函館市五稜郭町1-14　住友生命五稜郭ビル3F
	道東支店	0155-25-4892	080-0013	帯広市西三条南10-32　日本生命帯広駅前ビル5F
	小樽営業所	0134-24-5685	047-0036	小樽市長橋3-4-14
青森	青森支店	017-739-8501	030-0113	青森市第二問屋町4-1-20 NECソフトウェア青森本社ビル1F
	八戸営業所	0178-44-4354	031-0081	八戸市柏崎1-10-2　八戸第一生命ビル1F
	弘前営業所	0172-34-9083	036-8002	弘前市駅前2-2-2　弘前第一生命ビル1F
岩手	盛岡支店	019-635-3011	020-0866	盛岡市本宮3-13-20
	一関営業所	0191-25-6531	021-0041	一関市赤荻字月町218-2
宮城	仙台支店	022-292-1900	983-0852	仙台市宮城野区榴岡3-4-18　タカノボル22ビル4F
秋田	秋田支店	018-863-7938	010-0951	秋田市山王1-3-29
山形	山形支店	023-631-3502	990-2445	山形市南栄町3-6-34
	鶴岡営業所	0235-25-8386	997-0014	鶴岡市大宝寺町1-30
	米沢営業所	0238-24-1418	992-0027	米沢市駅前3-5-22　かなつビル1F
福島	郡山支店	024-938-5209	963-8022	郡山市西ノ内1-22-13
	福島支店	024-536-3703	960-8074	福島市西中央5丁目6番1号
	いわき営業所	0246-29-5301	970-8034	いわき市平上荒川字桜町34-1
	会津若松営業所	0242-28-1627	965-0818	会津若松市東千石2-1-45
茨城	鹿島営業所	0299-82-4860	314-0014	鹿嶋市光3　住友金属構内
	つくば支店	029-860-2002	305-0821	つくば市春日3-22-8
	水戸支店	029-257-1860	310-0911	水戸市見和3-575-3
栃木	宇都宮支店	028-632-8140	321-0954	宇都宮市元今泉2-7-6
	小山営業所	0285-21-1495	323-0807	小山市城東1-14-12　ウエルストン1ビル1F
群馬	群馬支店	027-243-6316	371-0026	前橋市大手町2-6-20　明治安田生命前橋ビル5F
	高崎営業所	027-365-3500	370-0073	高崎市緑町1-22-5
	太田営業所	0276-45-0666	373-0853	太田市浜町58-24

都道府県名	拠点名	電話番号	郵便番号	所在地
埼玉	大宮支店	048-660-1881	331-0812	さいたま市北区宮原町2-85-5
	熊谷営業所	048-527-0597	360-0036	熊谷市桜木町1-1-1　秩父鉄道熊谷ビル4F
	浦和支店	048-866-5471	336-0022	さいたま市南区白幡4-12-19
	川口営業所	048-225-6722	332-0001	川口市朝日6-2-3　あいおい損保・川口東ビル4F
	川越支店	04-2955-7695	350-1331	狭山市新狭山2-11-10
	越谷営業所	048-978-9500	343-0042	越谷市千間台東1-7-25　エムケービル1F
千葉	千葉支店	043-252-4309	260-0045	千葉市中央区弁天1-5-1　白樺ビル5F
	千葉東支店	043-221-6964	260-0843	千葉市中央区末広1-12-15
	成田営業所	0476-22-5390	286-0044	成田市不動ヶ岡2152-2　成田旭ビル1F
	君津営業所	0439-55-7278	299-1144	君津市東坂田1-3-2　京葉君津ビル3F
	船橋支店	047-434-1611	273-0012	船橋市浜町2-1-1　ららぽーと三井ビル1F
	柏営業所	0471-35-2400	277-0827	柏市松葉町2-5-1
	印西営業所	0476-46-4250	270-1352	印西市大塚1-9 千葉ニュータウンエネルギーセンター1F
東京	東京中央支店	03-3456-5213	108-0073	港区三田1-4-28　三田国際ビル1F
	大森支店	03-3764-0007	140-0013	品川区南大井6-25-3　ビリーヴ大森ビル8F
	五反田支店	03-3443-7905	141-0022	品川区東五反田5-25-16　朝日生命五反田ビル1F
	新橋支店	03-3431-9868	105-0012	港区芝大門2-5-5　住友芝大門ビル5F
	赤坂支店	03-5413-1701	107-0052	港区赤坂4-9-6　タク赤坂ビル2F
	三田支店	03-3452-6168	108-0073	港区三田1-4-28　三田国際ビル1F
	渋谷支店	03-5458-3341	150-0036	渋谷区南平台町2-17　日交渋谷南平台ビル8F
	新宿支店	03-3352-8071	160-0022	新宿区新宿4-2-18　新宿光風ビル3F
	池袋支店	03-3985-3194	170-0013	豊島区東池袋1-32-7　三井生命池袋ビル4F
	日本橋支店	03-3297-0783	104-0032	中央区八丁堀4-5-8　ノワール八丁堀2F
	江東支店	03-3649-3230	135-0016	江東区東陽2-2-20　住友不動産東陽駅前ビル1F
	秋葉原支店	03-5821-2474	111-0052	台東区柳橋2-19-6　秀和柳橋ビル8F
	足立営業所	03-3888-7151	120-0034	足立区千住1-11-2　カーニープレイス千住7F
	神田支店	03-3233-2411	101-0064	千代田区猿楽町2-7-8　住友水道橋ビル8F
	府中支店	042-362-6833	183-0036	府中市日新町1-4-5　第六MKビル1F
	立川支店	042-527-2527	190-0022	立川市錦町2-4-6　住友生命立川ビル3F
	小金井支店	042-385-7666	184-0013	小金井市前原町5-9-7
神奈川	神奈川支店	045-314-7625	220-0004	横浜市西区北幸2-8-4　横浜西口KNビル1F
	横須賀営業所	0468-27-3188	238-0004	横須賀市小川町14-1　ニッセイ横須賀センタービル1F
	川崎営業所	044-244-1083	210-0011	川崎市川崎区富士見1-6-3　B2棟3F
	相模原支店	042-746-6111	228-0803	相模原市相模大野7-1-6　相模大野第一生命ビル4F
	厚木支店	046-225-0411	243-0032	厚木市恩名900-4
	平塚支店	0463-21-4777	254-0035	平塚市宮の前1-2　あいおい損保平塚第一ビル2F
	藤沢営業所	0466-22-0204	251-0055	藤沢市南藤沢17-10　コア湘南田村ビル１Ｆ
	小田原営業所	0465-35-6647	250-0042	小田原市荻窪362　第二オギクボビル1F
	玉川支店	044-814-1551	213-0002	川崎市高津区二子5-1-1　高津パークプラザビル4F
新潟	新潟支店	025-243-2315	950-0983	新潟市神道寺275-3
	長岡営業所	0258-35-5217	940-0034	長岡市福住2-3-6　小林石油ビル
	柏崎地区センター	0257-22-2362	945-0833	柏崎市若葉町2-22　柏崎情報開発センター2F
富山	富山支店	076-442-2605	930-0004	富山市桜橋通り1-18　住友生命富山ビル1F
	黒部営業所	0765-54-0447	938-0031	黒部市三日市字新光寺1880-1
	高岡営業所	0766-25-4212	933-0912	高岡市丸の内1-40　高岡商工ビル8F
石川	金沢支店	076-223-3188	920-0864	金沢市高岡町1-39　住友生命金沢高岡町ビル1F
	小松営業所	0761-24-3782	923-0926	小松市龍助町36　小松東京海上ビル3F
	七尾営業所	0767-54-0298	926-0801	七尾市昭和町51-2
福井	福井支店	0776-54-6637	918-8206	福井市北四ツ居町518
山梨	甲府支店	055-226-7564	400-0858	甲府市相生2-3-16　住友海上甲府ビル3F
	富士吉田営業所	0555-23-9515	403-0005	富士吉田市上吉田3726　ヤマナシ文具センタービル2F

都道府県名	拠点名	電話番号	郵便番号	所在地
長野	松本支店	0263-27-7070	399-0033	松本市笹賀6096-1
	岡谷営業所	0266-24-4870	394-0028	岡谷市本町4-5-18
	長野支店	026-224-0050	380-0824	長野市南石堂町1293　清水長野ビル1F
	上田営業所	0268-27-6336	386-0032	上田市諏訪形5-1　豊成ビル5F
	飯田営業所	0265-53-7043	395-0815	飯田市松尾常盤台73-10
岐阜	東濃営業所	0572-55-4578	509-5132	土岐市泉町大富261-8
	岐阜支店	058-275-8801	500-8367	岐阜市宇佐南3-4-7
	高山営業所	0577-33-6524	506-0021	高山市名田町5-95-2　第3みたかビル5F
	中濃営業所	0574-27-6431	505-0041	美濃加茂市太田町飛鹿1927-2
静岡	静岡支店	054-202-6120	422-8061	静岡市森下町1-35　静岡MYタワー2F
	富士営業所	0545-64-6735	416-0944	富士市横割1-17-24　FCビル2F
	沼津支店	0559-73-6001	411-0906	駿東郡清水町八幡88-1
	浜松支店	053-466-0205	435-0047	浜松市原島町111
	掛川営業所	0537-23-2181	436-0056	掛川市中央1-4-2　タウンビル3F
愛知	名古屋支店	052-264-7525	460-0007	名古屋市中区新栄2-28-22　NEC名古屋ビル5F
	名西営業所	052-442-7451	490-1111	海部郡甚目寺町大字甚目寺字山王22 （株）シーエスイー山王ビル
	名南支店	052-694-1031	457-0862	名古屋市南区内田橋1-8-5　アートライフ・タケセイ1F
	半田営業所	0569-22-2762	475-0903	半田市出口町1-130-1　森田ビル4F
	小牧支店	0568-75-5594	485-0029	小牧市中央1-271　大垣共立銀行小牧支店ビル4F
	豊田営業所	0565-34-1168	471-0034	豊田市小坂本町1-5-3　朝日生命新豊田ビル4F
	三河支店	0564-23-5020	444-0044	岡崎市康生通南3-5　住友生命岡崎第二ビル1F
	豊橋営業所	0532-55-3063	440-0084	豊橋市下地町瀬上83
三重	三重支店	059-227-1622	514-0042	津市新町3-2-1
	四日市営業所	0593-51-0425	510-0075	四日市市安島1-5-10　明治安田生命四日市西浦ビル2F
	伊賀上野営業所	0595-23-8914	518-0873	上野市丸之内128　共立ビル2F
滋賀	滋賀支店	077-525-3156	520-0043	大津市中央4-5-4　BKビル
	彦根営業所	0749-24-1784	522-0073	彦根市旭町8-20
	八日市営業所	0748-25-0680	527-0022	八日市市上之町2-7　ウイング八日市3F
京都	京都支店	075-812-5800	604-8804	京都市中京区壬生坊城町24-1　古川勘ビル4F
	宇治営業所	0774-20-1210	611-0042	宇治市小倉町久保111-1　辻岩ビル新館4F
	福知山支店	0773-23-6287	620-0000	福知山市駅南町3-6　竹下駅南ビル1F
	舞鶴営業所	0773-63-7236	625-0036	舞鶴市字浜160　スクウェアービル大門3F
	亀岡営業所	0771-25-7320	621-0805	亀岡市安町中畠1-2　スカイビル7F
大阪	大阪中央支店	06-6264-2834	541-0053	大阪市中央区本町2-1-6　堺筋本町センタービル5F
	寝屋川支店	072-833-5284	573-0094	枚方市南中振1-16-27　宅建ハウジングビル6F
	淀川支店	06-6305-5444	532-0011	大阪市淀川区西中島1-11-16　住友商事淀川ビル3F
	高槻支店	0726-73-5481	569-0071	高槻市城北町1-5-25　高槻FJYビル1F
	千里支店	06-6835-0017	560-0083	豊中市新千里西町1-2-2　住友商事千里ビル　南館2F
	東大阪支店	0729-24-6780	581-0803	八尾市光町1-61　嶋野・住友生命ビル7F
	南大阪支店	072-223-8595	590-0026	堺市向陵西町2-1-24
	泉南支店	0724-63-2190	598-0012	泉佐野市高松東1-10-37　泉佐野センタービル8F
兵庫	豊岡営業所	0796-24-0331	668-0043	豊岡市桜町15-1　幸栄ビル1F
	神戸支店	078-332-5431	650-0031	神戸市中央区東町126　神戸シルクセンタービル3F
	姫路支店	0792-89-2684	670-0948	姫路市北条宮の町113
	明石支店	078-914-0550	673-0892	明石市本町二丁目2番24号　明石東京海上ビルディング
奈良	奈良支店	0742-36-1161	630-8001	奈良市法華寺町219-1
	橿原営業所	0744-23-6240	634-0813	橿原市四条町277-1　シェ・ホーム・ヤマ2F
和歌山	和歌山支店	073-428-3222	640-8154	和歌山市六番丁5　和歌山第一生命ビル
鳥取	鳥取営業所	0857-28-6068	680-0911	鳥取市千代水4-97
	米子営業所	0859-22-8280	683-0805	米子市西福原2-1-1　YNT第10ビル2階
島根	山陰支店	0852-21-0988	690-0825	松江市学園1-18-5
	浜田営業所	0855-22-6092	697-0033	浜田市朝日町70-5　朝日第2ビル1F

都道府県名	拠点名	電話番号	郵便番号	所在地
岡山	岡山支店	086-246-9606	700-0976	岡山市辰巳19-102
	倉敷営業所	086-426-1371	710-0057	倉敷市昭和2-4-6　住友生命倉敷ビル2F
	津山営業所	0868-28-2649	708-0872	津山市平福181-15　カワシマ商事（株）本社ビル3Ｆ
広島	広島支店	082-248-4222	730-0042	広島市中区国泰寺町2-5-11　西橋屋ビル4F
	呉営業所	0823-21-5129	737-0051	呉市中央1-6-9　日本団体生命ビル6F
	東広島営業所	0824-22-6411	739-0003	東広島市西条町大字土与丸441-1
	三次営業所	0824-63-3186	728-0013	三次市十日市東6-13-14
	福山支店	0849-31-8907	721-0973	福山市南蔵王町3-13-12
	備後府中営業所	0847-46-4835	726-0003	府中市元町475-1　カルチャープラザ4F
	尾道営業所	0848-22-3736	722-0037	尾道市西御所町14-15　第六堀田ビル4F
山口	山口支店	083-973-1858	754-0011	吉敷郡小郡町御幸町4-9　山陽ビル小郡1F
	周南営業所	0834-31-4114	745-0063	周南市今住町3-18
	岩国営業所	0827-22-9534	740-0018	岩国市麻里布町1-5-26　岩国通運ビル2F
	下関営業所	0832-53-3230	751-0853	下関市川中豊町2-6-36
	萩地区センター	0838-22-7472	758-0022	萩市浜崎町121-1　Kビル2F
徳島	徳島支店	088-622-1270	770-0852	徳島市徳島町2-19-1　あいおい損保徳島ビル4F
香川	高松支店	087-833-1771	760-0008	高松市中野町29-2　NEC四国ビル7F
	丸亀営業所	0877-23-8563	763-0034	丸亀市大手町3-5-18　ジブラルタ丸亀ビル7F
愛媛	松山支店	089-945-4145	790-0878	松山市勝山町1-19-3　青木第一ビル5Ｆ
	八幡浜営業所	0894-24-6158	796-0031	八幡浜市江戸岡一丁目4-6　江戸岡ビル2F
	宇和島営業所	0895-25-1000	798-0032	宇和島市恵美須町2-4-14　井上ビル
	今治営業所	0898-31-5741	794-0063	今治市片山1-2-20
	新居浜支店	0897-34-4774	792-0003	新居浜市新田町3-2　住友商事新居浜ビル5F
	川之江営業所	0896-24-3855	799-0113	川之江市妻鳥町1010番地8　共和ビル102号室
高知	高知支店	088-883-8884	780-0072	高知市杉井流70-5　マノワール杉井流
福岡	福岡支店	092-472-2853	812-0004	福岡市博多区榎田2-3-27　STS第二ビル3F
	福岡中央営業所	092-472-2853	812-0004	福岡市博多区榎田2-3-27　STS第二ビル3F
	博多営業所	092-472-2853	812-0004	福岡市博多区榎田2-3-27　STS第二ビル3F
	福岡東営業所	092-472-2853	812-0004	福岡市博多区榎田2-3-27　STS第二ビル3F
	北九州支店	093-522-0581	802-0014	北九州市小倉北区砂津1-5-34　小倉興産23号館4F
	飯塚営業所	0948-24-0919	820-0005	飯塚市新飯塚13-11　北代ビル2F
	久留米支店	0942-44-5298	839-0807	久留米市東合川町2-4-29
	大牟田営業所	0944-51-2655	836-0843	大牟田市不知火町2-7-1　中島物産ビル5F
佐賀	佐賀支店	0952-31-9301	849-0937	佐賀市鍋島3-2-19
	佐賀西営業所	0954-22-6567	843-0022	武雄市武雄町大字武雄5014-1　東洋リーセントビル5F
長崎	長崎支店	095-838-4442	851-0134	長崎市田中町586-7
	佐世保営業所	0956-22-2779	857-0043	佐世保市天満町3-23
	諫早営業所	0957-23-0471	854-0016	諫早市高城町5-15　諫早商工会館5F
熊本	熊本支店	096-383-6777	862-0925	熊本市保田窪本町1-40
大分	大分支店	097-503-2555	870-0921	大分市萩原4-9-65
	中津営業所	0979-23-1182	871-0058	中津市豊田町2-423-10　6 BILL 5F
宮崎	宮崎支店	0985-27-4477	880-0806	宮崎市広島1-18-7　大同生命宮崎ビル9F
	延岡営業所	0982-35-7545	882-0872	延岡市愛宕町2-1-12　センコービルディング5F
	都城営業所	0986-23-4821	885-0021	都城市平江町13街区15　富士火災海上保険ビル3F
鹿児島	鹿児島支店	099-285-2266	890-0062	鹿児島市与次郎2-4-35　KSC鴨池ビル1F
	出水営業所	0996-62-8922	899-0202	出水市昭和町13-1　第二丸久ビル2F
沖縄	沖縄支店	098-876-2788	901-2132	浦添市伊祖2-7-11

用語解説

3DES：triple-DES
DESによる暗号化を3回行うもので、DESよりも暗号強度が高くなっています。

AES：Advanced Encryption Standard
AESは、DESに代わる暗号アルゴリズムとして急速に普及しています。 AESは3DESやDESよりも強力で高速であるため、 DES、3DESの両方の置き換えとして使うことができます。

AH: Authentication Header(認証ヘッダ)
IPSecで定義されるプロトコルです。IPヘッダを含めて認証を行い、転送中にパケットの内容が改ざんされていないことを確認します。

Cookie
ウェブサーバが指定するウェブクライアントの情報でウェブクライアントの端末に保存されます。再度ウェブサーバにアクセスするとき保存した情報がHTTPヘッダに書き込まれる仕組みになっています。

DDoS：Distributed DoS
クラッキング手法の1つです。ネットワークに分散する多数の端末から、一斉に目標のサーバへパケットを送信し、サーバを過負荷に陥れてサービスを停止させたり、通信路をあふれさせたりする攻撃です。クラッカーは、あらかじめ攻撃対象のサーバと関連のない多くの端末に侵入して、ある条件をもとに一斉に攻撃を仕掛けるようなプログラムを埋め込ませておきます。

DES：Data Encryption Standard
アメリカの技術標準を定める政府機関において標準化された秘密鍵の暗号化形式です。秘密裏に交換された鍵を交換する方式で、56ビット長の鍵を利用します。

DMZ：DeMilitarized Zone
非武装地帯とも呼ばれ、内部ネットワークと外部ネットワークとの狭間に追加されたネットワークです。通常、外部に公開するサーバ群を配し、外部ネットワークから内部ネットワークへの通信を行わない構成とするときに用いられます。

DNS：Domain Name System
ドメイン名とIPアドレスを対応させるシステムです。

DoS：Denial of Service
クラッキング手法の1つです。ある端末から目標のサーバに過剰なパケットを送信し、サーバを過負荷に陥れてサービスを停止したり、通信路をあふれさせたりする攻撃です。

ESP: Encapsulating Security Payload
(暗号化ペイロード)
IPパケットの内容を暗号化するときに用いられるIPSecヘッダです。IPヘッダを除いて暗号化、認証を行います。

FTP：File Transfer Protocol
(ファイル転送プロトコル)
FTPサーバを介してファイルのやり取りを行うためのプロトコルです。

HTTP：Hyper Text Transfer Protocol
(ハイパーテキスト転送プロトコル)
ウェブサーバとウェブクライアント間でデータをやり取りするためのプロトコルです。

ICMP：Internet Control Message Protocol
(インターネット制御メッセージプロトコル)
ネットワーク機器間で互いの状態を確認するためにIPのエラーメッセージや制御メッセージを転送するプロトコルです。

IKE：Internet Key Exchange
(インターネット鍵交換)
IPSecによる暗号化通信の前に通信相手の認証、暗号化アルゴリズム、鍵の取り決めを行うためのプロトコルです。

IPSec：IP Security
IPパケットを暗号化するためのしくみです。まずIKEを利用して通信相手の通信相手の認証、暗号化アルゴリズム、暗号鍵の交換を行い、それをもとに暗号通信を行います。さらにデータが本物の通信相手からのものであるか、データの改ざんはないかどうかについて認証を行います。

IPアドレス
ネットワークに接続された端末や機器を識別するためのアドレスです。

JavaScript
Webブラウザ向けのJavaに似たプログラミング言語です。

MD5：Message Digest5
ハッシュアルゴリズムの1つです。128ビットのハッシュに圧縮します。

NAT：Network Address Translation
(ネットワークアドレス変換)
IPアドレスを変換する機能です。

NAPT：Network Address Port Translation
(ネットワークアドレスポート変換)
NAT機能を拡張したもので、ポート番号を利用して複数の内部IPアドレスを外部IPアドレスに動的に変換する機能です。IPマスカレードとも呼びます。

PFS：Perfect Forward Secrecy
ある鍵が解読されたとしても、その解読された鍵情報からは、その後に生成された別の鍵が解読できない性質を言います。

Ping Sweep
ある一定の範囲のIPアドレスに対してPingを発行し、応答するIPアドレスを発見するために用いられる手法です。攻撃を仕掛ける前の事前調査活動として利用されることが多いです。

RSA: Rivest Shamir Adleman
公開鍵暗号方式の暗号化アルゴリズムの1つです。Rivest氏、Shamir氏、Adleman氏が共同で開発しました。

SA: Security Association
(セキュリティアソシエーション)
IPSecで定義され、情報を保護するためのポリシーと暗号化に用いる鍵のセットで、トンネルを一意に特定し、リンクします。

SHA-1：Secure Hash Algorithm1
ハッシュアルゴリズムの1つです。160ビットのハッシュに圧縮します。

SMTP：Simple Mail Transfer Protocol
(簡易メール送信プロトコル)
電子メールを送信するためのプロトコルです。

SPI：Security Parameter Index
IPSecで定義されるSAを一意に特定するためのIDです。

SYN
TCPの制御ビットの1つです。通信相手とのコネクション確立時にSYNビットをオンにしたパケットを送信します。

SYN Flood
DoS攻撃の1つです。攻撃者は適当なIPアドレス、あるいはネットワーク上のターゲットホストのIPアドレスを送信元としてSYNパケットを大量にターゲットに送信します。

TCP：Transmission Control Protocol
(伝送制御プロトコル)
HTTP、SMTP、FTPなどの通信に利用されるプロトコルで、通信の信頼性を確保する仕組みを備えています。

traceroute
ICMPやUDPを用いて通信相手までの通信経路確認を行うために利用するコマンドの総称です。

UDP：User Datagram Protocol
DNS、DHCPなどで利用されるプロトコルで、通信制御は行わないが処理が少ない分低負荷で通信が行えます。

VPN：Virtual Private Network
(仮想専用線)
通信相手との間に構築された仮想的なプライベートネットワークです。インターネットを介しながらも独立したネットワークを利用しているかのように通信することができます。

暗号化ペイロード
→ESP（Encapsulating Security Payload）

共有鍵
あらかじめ相手と共有している鍵です。IKEの手順を踏まずにIPSec通信が行えます。

公開鍵
暗号鍵と復号鍵に異なる鍵を利用する暗号通信方式を公開鍵暗号通信方式と呼びます。公開鍵通信方式ではどちらかの鍵を公開し、もう一方の鍵を本人だけの秘密にします。公開されているほうの鍵を公開鍵と呼びます。

サブネットマスク
IPアドレスのネットワークアドレスとホストアドレスの区切りを指定するための値です。例えば、192.168.1.1/24というアドレスならば、24ビット目までがネットワークアドレスとなり、残りの8ビットがホストアドレスとなります。

自動鍵
IKEによって生成する鍵です。

セキュリティアソシエーション
→SA（Security Association）

トランスポートモード
IPSecにおけるモードの1つです。ホスト間の通信で利用されるモードで、トンネルモードのように新しいヘッダを付加することはありません。

トンネルモード
IPSecにおけるモードの1つです。ゲートウェイ間、あるいはゲートウェイ対ホスト間で利用されるモードで、新しいヘッダを付け加えます。

認証ヘッダ
→AH（Authentication Header）

秘密鍵
公開鍵暗号通信方式において自分だけの秘密にしておく鍵を秘密鍵と呼びます。

プロキシ
内部ネットワークの各端末の通信を代理で実行する機器、またはプログラムのことです。外部ネットワークから内部ネットワークへの通信、内部ネットワークから外部ネットワークへの通信を制御するときに有効です。

ポート番号
HTTP、SMTP、FTPなどの通信種別を判別するために用いられる番号です。通常サーバにはあらかじめ決められたポート番号を設定します。クライアントには自動的に空いている番号が割り当てられます。

索　引

記号

A

B

C

D

E

F

I

L

M

N

P

R

S

T

U

V

ア

カ

サ

タ

ナ

ハ

マ

ヤ

ラ

ワ

The BSD Copyright

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it toyour programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps:(1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program(independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program(or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.
Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANYKIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the
library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

■ 謝辞

Linus Torvalds氏をはじめとするLinuxに関わるすべての皆様に心より感謝いたします。

NEC Express5800 サーバ
Express5800 シリーズ
InterSec
N8100-1017

Express5800/SG300b

ユーザーズガイド
2005 年　3 月　　初版

日　本　電　気　株　式　会　社
東京都港区芝五丁目 7 番 1 号
TEL（03）3454-1111 （大代表）

乱丁・落丁はお取り替えいたします。

<本装置の利用目的について>

本製品は、高速処理が可能であるため、高性能コンピュータの平和的利用に関する日本政府の指導対象になっております。
ご使用に際しましては、下記の点につきご注意いただけますよう、よろしくお願いいたします。

1. 本製品は不法侵入、盗難等の危険がない場所に設置してください。
2. パスワード等により適切なアクセス管理をお願いいたします。
3. 大量破壊兵器およびミサイルの開発、ならびに製造等に関わる不正なアクセスが行われるおそれがある場合には、事前に弊社相談窓口までご連絡ください。
4. 不正使用が発覚した場合には、速やかに弊社相談窓口までご連絡ください。

弊社相談窓口　　ファーストコンタクトセンター
電話番号　03-3455-5800

注　意

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に接近して使用されると電波妨害を引き起こすことがあります。本書に従って正しい取り扱いをしてください。

高調波適合品

この装置は、高調波電流規格 JIS C 61000-3-2適合品です。
：JIS C 61000-3-2適合品とは、日本工業規格「電磁両立性－第3-2部：限度値－高調波電流発生限度値（1相当たりの入力電流が20A以下の機器）」に基づき、商用電力系統の高調波環境目標レベルに適合して設計・製造した製品です。

回線への接続について

本体を公衆回線や専用線に接続する場合は、本体に直接接続せず、技術基準に適合し認定されたボードまたはモデム等の通信端末機器を介して使用してください。

電源の瞬時電圧低下対策について

この装置は、落雷等による電源の瞬時電圧低下に対し不都合が生じることがあります。電源の瞬時電圧低下対策としては、交流無停電電源装置（UPS）等を使用されることをお勧めします。

レーザ安全基準について

この装置に標準で搭載されている光磁気ディスクドライブは、レーザに関する安全基準（JIS C-6802、IEC 60825-2）クラス1に適合しています。

海外でのご使用について

この装置は、日本国内での使用を前提としているため、海外各国での安全規格等の適用を受けておりません。したがって、この装置を輸出した場合に当該国での輸入通関および使用に対し罰金、事故による補償等の問題が発生することがあっても、弊社は直接・間接を問わず一切の責任を免除させていただきます。